

Reference Guide

AVAYA P330-ML-ML

STACKABLE SWITCH

SOFTWARE VERSION 4.5

Contents

Chapter 1	Using the CLI.....	1
	CLI Architecture.....	1
	Conventions Used.....	2
	CLI Help.....	2
	Command Line Prompt.....	2
	Navigation, Cursor Movement and Shortcuts.....	2
	Command Syntax.....	3
	Command Abbreviations.....	3
	Universal Commands.....	4
	Top and Up commands.....	4
	Retstatus command.....	4
	Tree command.....	4
	P330-ML Sessions.....	4
	Security Levels.....	6
	Entering the Supervisor Level.....	6
	Entering the CLI.....	7
	Entering the Technician Level.....	7
	Warranty.....	7
	Notice.....	7
	Avaya Support.....	7
Chapter 2	Avaya P330-ML Layer 2 CLI Commands.....	9
	clear cam.....	9
	clear dot1x config.....	9
	clear dynamic vlans.....	10
	clear log.....	10
	clear logging file.....	10
	clear logging server.....	11
	clear port mirror.....	11
	clear port static-vlan.....	12
	clear radius authentication server.....	12
	clear rmon statistics.....	12
	clear screen.....	13
	clear secure mac.....	13
	clear snmp trap.....	14
	clear timezone.....	14
	clear utilization cpu.....	14
	clear vlan.....	15
	copy module-config scp.....	15

copy module-config tftp	16
copy running-config scp	17
copy running-config startup-config	18
copy running-config tftp	18
copy scp module-config	19
copy scp stack-config	20
copy scp startup-config	22
copy stack-config scp	23
copy stack-config tftp	24
copy startup-config scp	25
copy startup-config tftp	25
copy tftp EW_archive	26
copy tftp module-config	27
copy tftp stack-config	27
copy tftp startup-config	28
copy tftp SW_image	29
copy tftp SW_powerinline_image	31
crypto key generate dsa	31
dir	32
disconnect ssh	33
get time	34
help	34
hostname	35
ip access-list	35
ip access-list-cookie	37
ip access-list-copy	37
ip access-default-action	38
ip access-list-dscp operation	38
ip access-list-dscp trust	39
ip access-list-name	40
ip access-list-owner	40
ip http enable	41
ip icmp redirect	41
ip simulate	41
ip ssh enable	42
ip telnet enable	42
ip telnet-client enable	43
no ip http	43
no ip icmp redirect	43
no ip ssh	44
no ip telnet	44
no ip telnet-client	44
no rmon alarm	45
no rmon event	45

no rmon history	46
no snmp-server	46
no snmp-server engineID	46
no snmp-server community	47
no snmp-server group	47
no snmp-server host	48
no snmp-server notifications	49
no snmp-server remote-user	49
no snmp-server user	49
no snmp-server view	50
no username	50
nvrn initialize	51
ping	51
prompt-length	52
reset	52
reset mgp	53
reset stack	54
reset wan	54
retstatus	54
rmon alarm	55
rmon event	56
rmon history	56
session	57
set allowed managers	58
set allowed managers ip	58
set arp-aging-interval	59
set arp-tx-interval	59
set autopartition	60
set boot bank	60
set cascading	61
set device-mode	61
set dot1x max-req	61
set dot1x quiet-period	62
set dot1x re-authperiod	62
set dot1x server-timeout	62
set dot1x supp-timeout	63
set dot1x system-auth-control disable	63
set dot1x system-auth-control enable	64
set dot1x tx-period	64
set inband vlan	65
set intelligent-multicast	65
set intelligent-multicast client-port-pruning time	65
set intelligent-multicast group-filtering-delay time	66
set intelligent-multicast router-port-pruning time	66

set interface inband	67
set interface ppp	67
set interface ppp enable/enable-always/disable/off/reset	68
set intermodule port redundancy	69
set intermodule port redundancy off	70
set internal buffering	70
set ip route	71
set license	71
set logging file condition	72
set logging file disable	74
set logging file enable	74
set logging server	74
set logging server access-level	75
set logging server condition	75
set logging server disable	77
set logging server enable	77
set logging server facility	78
set logging session condition	79
set logging session disable	80
set logging session enable	80
set logout	81
set mac-aging	81
set mac-aging-time	82
set port auto-negotiation-flowcontrol-advertisement	82
set port channel	83
set port classification	84
set port disable	84
set port dot1x initialize	85
set port dot1x max-req	85
set port dot1x port-control	86
set port dot1x quiet-period	86
set port dot1x re-authenticate	87
set port dot1x re-authentication	87
set port dot1x re-authperiod	88
set port dot1x server-timeout	88
set port dot1x supp-timeout	89
set port dot1x tx-period	89
set port duplex	89
set port edge admin state	90
set port enable	91
set port flowcontrol	91
set port level	92
set port mirror	93
set port name	94

set port negotiation	94
set port point-to-point admin status	95
set port powerline	96
set port powerline priority	96
set port redundancy	97
set port redundancy on/off	97
set port redundancy-intervals	98
set port security	99
set port spantree cost	99
set port spantree disable	100
set port spantree enable	100
set port spantree force-protocol-migration	100
set port spantree priority	101
set port speed	101
set port static-vlan	102
set port trap	103
set port vlan	103
set port vlan-binding-mode	104
set powerinline external power	105
set ppp authentication incoming	105
set ppp baud-rate	106
set ppp chap-secret	106
set ppp incoming timeout	106
set psu type	107
set qos policy-source	107
set queuing scheme	108
set radius authentication enable/disable	108
set radius authentication retry-number	109
set radius authentication retry-time	109
set radius authentication secret	110
set radius authentication server	110
set radius authentication udp-port	110
set secure mac	112
set security mode	112
set security violation	112
set snmp community	113
set snmp retries	113
set snmp timeout	114
set snmp trap	114
set snmp trap auth	115
set spantree default-path-cost	116
set spantree disable	116
set spantree enable	116
set spantree forward-delay	117

set spantree hello-time	117
set spantree max-age	118
set spantree priority	118
set spantree tx-hold-count	119
set spantree version	119
set system contact	120
set system location	120
set system name	121
set terminal recovery password disable	121
set terminal recovery password	121
set time client	122
set time protocol	122
set time server	123
set timezone	123
set trunk	124
set utilization cpu	124
set vlan	125
set web aux-files-url	125
set welcome message	126
show allowed managers status	127
show allowed managers table	127
show arp-aging-interval	128
show arp-tx-interval	128
show autopartition	129
show boot bank	130
show cam	130
show cam mac	131
show cam vlan	131
show cascading fault-monitoring	132
show copy status	133
show dev log file	133
show device-mode	134
show dot1x	134
show download status	134
show erase status	135
show image version	135
show intelligent-multicast	136
show intelligent-multicast hardware-support	136
show interface	137
show intermodule port redundancy	137
show internal buffering	137
show ip access-group	138
show ip access-list details	138
show ip access-list-dscp	139

show ip access lists	140
show ip access-list-summary	141
show ip route	141
show ip ssh	142
show l2-module-config	142
show l2-stack-config	145
show license	148
show log	149
show logging file condition	150
show logging file content	151
show logging server condition	153
show logging session condition	154
show logout	154
show mac-aging	154
show mac-aging-time	155
show module	155
show module-identity	156
show port	157
show port auto-negotiation-flowcontrol-advertisement	158
show port channel	158
show port classification	160
show port dot1x	161
show port dot1x statistics	163
show port edge state	164
show port flowcontrol	164
show port mirror	166
show port point-to-point status	166
show port redundancy	167
show port security	167
show port trap	168
show port vlan-binding-mode	168
Show powerinline	169
show powerinline image version	170
show ppp authentication	171
show ppp baud-rate	172
show ppp configuration	172
show ppp incoming timeout	172
show ppp session	173
show protocol	173
show queuing scheme	174
show radius authentication	174
show rmon alarm	175
show rmon event	176
show rmon history	176

show rmon statistics	177
show secure current	178
show secure mac	178
show security mode	179
show snmp	179
show snmp engineID	181
show snmp group	182
show snmp retries	184
show snmp timeout	184
show snmp user	184
show snmp userToGroup	185
show snmp view	186
show spantree	188
show system	191
show tftp download software status	192
show time	192
show time parameters	193
show timeout	193
show timezone	193
show trunk	194
show upload status	195
show username	196
show utilization	196
show vlan	198
show web aux-files-url	199
snmp-server community	199
snmp-server enable	200
snmp-server enable notifications	200
snmp-server engineID	200
snmp-server group	201
snmp-server host	202
snmp-server informs	203
snmp-server remote-user	204
snmp-server user	205
snmp-server view	206
stack health	206
sync time	207
tech	207
telnet	207
terminal	208
username	208
validate-group	209
Chapter 3 Avaya P330-ML Layer 3 CLI Commands	211
How the Layer 3 CLI is Organized	211

Router Configuration Contexts	211
Shortcuts to Commands by Context	211
General Commands	212
arp	212
arp timeout	212
clear arp-cache	213
clear fragment	214
clear ip route	214
clear ip traffic	215
clear screen	215
clear vlan	215
configure	216
copy module-config scp	216
copy module-config tftp	216
copy running-config scp	217
copy running-config startup-config	218
copy running-config tftp	218
copy scp module-config	219
copy scp startup-config	220
copy startup-config scp	220
copy startup-config tftp	221
copy tftp startup-config	221
disconnect ssh	222
erase startup-config	222
event log	223
exit	223
fragment chain	224
fragment size	224
fragment timeout	225
help	225
hostname	226
icmp in-echo-limit	226
interface	227
ip access-default-action	227
ip access-group	228
ip access-list	228
ip access-list-cookie	229
ip access-list-copy	230
ip access-list-dscp operation	230
ip access-list-dscp trust	231
ip access-list-name	232
ip access-list-owner	232
ip bootp-dhcp relay	233
ip default-gateway	234

ip max-arp-entries	234
ip max-route-entries	235
ip netmask-format	235
ip ospf router-id	236
ip route	237
ip routing	237
ip simulate	238
ping	239
prompt-length	239
reset	240
router ospf	240
router rip	241
router srrp	241
router vrrp	242
session	242
set device-mode	243
set policy type	244
set qos policy-source	244
set system contact	245
set system location	245
set system name	246
set vlan	247
show copy status	247
show device-mode	248
show download status	248
show erase status	248
show fragment	249
show ip access-group	250
show ip access-lists	250
show ip access-list-dscp	251
show ip access-list-summary	251
show ip arp	252
show ip icmp	253
show ip interface	253
show ip interface brief	254
show ip ospf	255
show ip ospf database	255
show ip ospf interface	256
show ip ospf neighbor	256
show ip protocols	257
show ip reverse-arp	258
show ip route	258
show ip route best-match	259
show ip route static	259

show ip route summary	260
show ip ssh	260
show ip srrp	260
show ip traffic	261
show ip unicast cache	263
show ip unicast cache networks	264
show ip unicast cache networks detailed	265
show ip unicast cache nextHop	266
show ip unicast cache summary	266
show ip vrrp	267
show ip vrrp detail	267
show policy type	268
show startup-config	270
show system	270
show upload status	271
show vlan	271
terminal	271
traceroute	272
validate-group	272
Interface Context	274
default-metric	274
enable vlan commands	274
ip address	275
ip admin-state	275
ip bootp-dhcp network	276
ip bootp-dhcp server	276
ip broadcast-address	277
ip directed-broadcast	277
ip netbios-rebroadcast	278
ip ospf authentication-key	278
ip ospf cost	279
ip ospf dead-interval	279
ip ospf hello-interval	279
ip ospf priority	280
ip proxy-arp	280
ip redirects	281
ip rip authentication key	281
ip rip authentication mode	282
ip rip default-route-mode	282
ip rip poison-reverse	283
ip rip rip-version	283
ip rip send-receive-mode	284
ip rip split-horizon	285
ip routing-mode	285

ip srrp backup	286
ip vlan/ip vlan name	286
ip vrrp	287
ip vrrp address	287
ip vrrp auth-key	288
ip vrrp override addr owner	288
ip vrrp preempt	289
ip vrrp primary	289
ip vrrp priority	290
ip vrrp timer	290
Router RIP Context	291
network	291
redistribute	291
timers basic	292
Router OSPF Context	293
area	293
network	293
passive-interface	294
redistribute	294
timers spf	295
Router SRRP Context	296
poll-interval	296
timeout	296
Index of Layer 2 CLI Commands	297
Index of Layer 3 CLI Commands	301

Using the CLI

This chapter describes the Avaya P330 CLI architecture and conventions, and provides instructions for accessing the Avaya P330 for configuration purposes.

The configuration procedure involves establishing a Telnet session or a serial connection and then using the Avaya P330's internal CLI.

The CLI is command-line driven and does not have any menus. To activate a configuration option, you must type the desired command at the prompt and press Enter.

You can also configure your Avaya P330 using the P330 Manager with its graphical user interface. For details, see the switch User's Guide and the Avaya™ MultiService Network Manager P330 Device Manager User's Guide on the Documentation and Utilities CD.

CLI Architecture

The P330 stack supports both Layer 2 switching and Layer 3 routing (Layer 3 functionality depends on the module type).

The P330 CLI includes two CLI entities to support this functionality.

- The Switch CLI entity is used to manage Layer 2 switching of the entire stack. The Switch CLI entity is identical to the CLI of a P330 Layer 2 modules. CLI commands for managing Layer 2 switching are described in Chapter 2.
- The Router CLI entity is used to manage Layer 3 routing of a single module. The Router CLI entity exists only in Layer 3 modules (P333R, P333R-LB and P330-ML). CLI commands for managing Layer 3 routing are described in Chapter 3.

If the Layer 3 module is the Stack Master, then the Switch CLI entity and the Router CLI entity co-exist on the same module.

To switch between the entities, use the **session** command.

Configuration of the **password** commands and **community** commands in one entity is automatically attributed to the other entity in the stack.

Initial access to the stack can be established via a serial connection or a Telnet connection to any one of the entities.

Conventions Used

The following conventions are used in this chapter to convey instructions and information:

- Mandatory keywords are in boldface.
- Variables that you supply are in pointed brackets <>.
- Optional keywords are in square brackets [].
- Alternative but mandatory keywords are grouped in braces {} and separated by a vertical bar |.
- If you enter an alphanumeric string of two words or more, enclose the string in inverted commas.
- Information displayed on screen is displayed in text font.

CLI Help

The CLI has its own Help utility. Use the following key sequences to operate the CLI Help:

- To display all commands available in a context type a question mark.
- To display all commands starting with a certain string, type the first few letters followed by a question mark.
- To get help containing all commands parameters with their legal values as well as its syntax and an example, type a question mark at the end of command or at the stage where it is unique.
- Use the Tab key to complete an unambiguous command.

Example: Router> **show?**

Command Line Prompt

Navigation, Cursor Movement and Shortcuts

The CLI contains a simple text editor with these functions:

Table 1.1 Navigation, Cursor Movement and Shortcuts

Keyboard	Functions
Backspace	Deletes the previous character
Up arrow/Down arrow	Scrolls back and forward through the command history buffer
Left arrow/Right arrow	Moves the cursor left or right

Table 1.1 Navigation, Cursor Movement and Shortcuts

Keyboard	Functions
Tab	Completes the abbreviated command. Type the minimum number of characters unique to the command. An exception is the Reset System command which you must type in full.
Enter	Executes a single-line command
“ ”	If you type a name with quotation marks, the marks are ignored.

Command Syntax

Commands are not case-sensitive. That is, uppercase and lowercase characters may be interchanged freely.

Command Abbreviations

All commands and parameters in the CLI can be truncated to an abbreviation of any length, as long as the abbreviation is not ambiguous. For example, `version` can be abbreviated `ver`.

For ambiguous commands, type the beginning letters on the command line and then use the Tab key to toggle through all the possible commands beginning with these letters.

Universal Commands

Universal commands are commands that can be issued anywhere in the hierarchical tree.

Top and Up commands

The `Up` command moves you up to the next highest level in the CLI command hierarchy. The `Top` command moves you to the highest level.

Retstatus command

Use the `retstatus` command to show whether the last CLI command you performed was successful. It displays the return status of the previous command.

The syntax for this command is: **retstatus**

Output Example:

```
P330 # set port negotiation 2/4 disable
Link negotiation protocol disabled on port 2/4.
```

Tree command

The `tree` command displays the commands that are available at your current location in the CLI hierarchy.

The syntax for this command is: **tree**

P330 Sessions

You can use `sessions` to switch between the CLI of P330 modules / other stack entities (for example, an X330 ATM or WAN entity plugged into a specific P330 switch or with the G700 Media Gateway Processor) or to switch between Layer 2 and Layer 3 commands in the router module.

To switch between P330 modules use the command:

```
session [<mod_num>] <mode>.
```

The `<mod_num>` is the number of the module in the stack, counting from the bottom up.

The `<mode>` can be either **switch**, **router**, **wan**, **atm**, **mgp**.

Use **switch** mode to configure layer 2 commands.

Use **router** mode to configure routing commands.

Examples:

To configure router parameters in the module that you are currently logged into, type the following command:

```
session router.
```

To configure the switch parameters, on module 6, type the command:
session 6 switch.



Note: When you use the `session` command the security level stays the same.



Note: Use the `session` command without any parameters to identify the stack master and its slot number. It will list all the modules in the stack and their slot number with the master module marked with an asterisk.

Security Levels

There are four security access levels – User, Privileged, Configure and Supervisor.

- The User level is a general access level used to show system parameter values.
- The Privileged level is used by site personnel to access stack configuration options.
- The Configure level is used by site personnel for Layer 3 configuration.
- The Supervisor level is used to define user names, passwords, and access levels of up to 10 local users.

A login name and password are always required to access the CLI and the commands. The login names and passwords, and security levels are established using the `username` command.

Switching between the entities, does not effect the security level since security levels are established specifically for each user. For example, if the operator with a privileged security level in the Switch entity switches to the Router entity the privileged security level is retained.

Entering the Supervisor Level

The Supervisor level is the level in which you first enter Cajun Campus CLI and establish user names for up to 10 local users. When you enter the Supervisor level, you are asked for a Login name. Type `root` as the Login name and the default password `root` (in lowercase letters):

```
Welcome to P330
Login: root
Password:****
Password accepted.
P330-N(super)#
```

Defining new users

Define new users and access levels using the `username` command in Supervisor Level.

Exiting the Supervisor Level

To exit the Supervisor level, type the command `exit`.

Entering the CLI

To enter the CLI, enter your username and password. Your access level is indicated in the prompt as follows:

The User level prompt is shown below:

```
P330-N>
```

The Privileged level prompt is shown below:

```
P330-N#
```

The Configure level prompt for Layer 3 configuration is shown below:

```
P330-N( configure )#
```

The Supervisor level prompt is shown below:

```
P330-N( super )#
```

Entering the Technician Level

This level is can only be accessed from the Privileged and Supervisor levels not from the User level.

This feature is not documented and is for use by Avaya Technical Support only.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement or other applicable documentation to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website: <http://www.avaya.com/support>.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com>

Avaya P330-ML Layer 2 CLI Commands

This chapter describes all the P330-ML Layer 2 CLI commands and parameters in alphabetical order.

clear cam

User level: privileged, supervisor.

Use the `clear cam` command to delete all entries from the CAM table.

The syntax for this command is:

```
clear cam
```

Example:

```
P330-N# clear cam  
  
CAM table cleared.
```

clear dot1x config

User level: supervisor

Use the `clear dot1x config` command to disable dot1x on all ports and return values to the default settings..

The syntax for this command is:

```
clear dot1x config
```

Example:

```
P330-N# clear dot1x config  
  
Original Configuration was Restored
```

clear dynamic vlans

User level: privileged, supervisor.

① This command is available on the P330-ML-ML only.

Use the `clear dynamic vlans` command to clear dynamically learned VLANs. Only the VLANs learned by the switch from incoming traffic are cleared using this command.

The syntax for this command is:

```
clear dynamic vlans
```

Example:

```
P330-N# clear dynamic vlans
This command will delete all the vlans that were
dynamically learned by the device - do you want to continue
(Y/N)? y

Dynamic vlans were deleted from device tables
```

clear log

User level: privileged, supervisor.

Use the `clear log` command to delete the log file of a switch.

The syntax for this command is:

```
clear log [<module>]
```

```
module          Number of switch (1...10)
(Optional)
```

Example:

```
P330-N# clear log
Cleared all logfiles.
```

clear logging file

User level: privileged, supervisor.

Use the `clear logging file` command to delete the log file and open an empty one.

The syntax for this command is:

```
clear logging file
```


Example:

```
P330-N>clear logging file
Done!
```

clear logging server

User level: privileged, supervisor.

Use the `clear logging server` command to delete a Syslog server from the Syslog server table.

The syntax for this command is:

```
clear logging server <ip-address>
```

`ip-address` The IP address of the Syslog server.

Example:

```
P330-N# clear logging server 149.49.38.22
Done!
```

clear port mirror

User level: privileged, supervisor.

Use the `clear port mirror` command to cancel port mirroring.

The syntax for this command is:

```
clear port mirror [<source module>/<source port>/<dest module>/<dest port>]
```

`source module` Source module number

`source port` Source port number

`dest module` Destination module number

`dest port` Destination port number

Example:

```
P330-N# clear port mirror 1/2/1/4
this command will delete the port mirror entry
- do you want to continue (Y/N)? y
Mirroring packets from port 1/2 to port 1/4 is cleared
```

clear port static-vlan

User level: privileged, supervisor.

Use the `clear port static-vlan` command to delete VLANs statically configured on a port.

The syntax for this command is:

```
clear port static-vlan [module/port range][vlan num]
```

module/port range	Port range
vlan num	The VLAN to unbind from the port

Example:

```
P330-N# clear port static-vlan 3/10 5  
VLAN 5 is unbound from port 3/10
```

clear radius authentication server

User level: supervisor

Removes a primary or secondary RADIUS authentication server.

The syntax for this command is:

```
clear radius authentication server [{primary|secondary}]
```

primary	Remove primary RADIUS server
secondary	Remove secondary RADIUS server

Example:

```
P330-1(super)# clear radius authentication server secondary
```

clear rmon statistics

User level: privileged, supervisor.

Use the `clear rmon statistics` command to clear the RMON statistics counter.

The syntax for this command is:

```
clear rmon statistics
```

Example:

```
P330-N# clear rmon statistics
cleared device counters
```

clear screen

User level: user, privileged, supervisor

Use the clear screen command to clear the current terminal display.

The syntax for this command is:

```
clear screen
```

clear secure mac

User level: user, privileged, supervisor

① If this command is to be implemented on a switch other than the stack master, a session should be opened to the relevant switch.

Use the `clear secure mac` command to remove a MAC address from the CAM table of a secured port.

The syntax for this command is:

```
clear secure mac <mac-address> port <mod-num>/<port-num>
```

mac-address	MAC address to be cleared
mod-num	Module where the secured port is located
port-num	Secured port number

Example:

```
P330-N# clear secure mac 00-10-5a-0f-5e-1c port 1/23
secure mac 00-10-5a-0f-5e-1c port 1/23 was removed.
```

clear snmp trap

User level: privileged, supervisor.

Use the `clear snmp trap` command to clear an entry from the SNMP trap receiver table.

The syntax for this command is:

```
clear snmp trap {<rcvr_addr>|all}
```

`rcvr_addr` IP address or IP alias of the trap receiver (the SNMP management station) to clear

`all` Keyword that specifies every entry in the SNMP trap receiver table

Example:

```
P330-N# clear snmp trap 192.168.173.42  
SNMP trap deleted.
```

clear timezone

User level: privileged, supervisor.

Use the `clear timezone` command to reset the time zone to its default value UTC (Coordinated Universal Time)

The syntax for this command is:

```
clear timezone
```

Example:

```
P330-N# clear timezone  
Timezone name and offset cleared.
```

clear utilization cpu

User level: privileged, supervisor.

Use the `clear utilization cpu` command to disable CPU utilization monitoring on the specified module.

The syntax for this command is:

```
clear utilization cpu <module-number>
```

module-number	The module number for which CPU utilization monitoring is disabled.
---------------	---

Example:

```
P330-N# clear utilization cpu 1
CPU utilization is cleared on module 1
```

clear vlan

User level: privileged, supervisor.

Use the `clear vlan` command to delete an existing VLAN and return ports from this VLAN to the default VLAN #1. When you clear a VLAN, all ports assigned to that VLAN are assigned to the default VLAN #1.

The syntax for this command is:

```
clear vlan [<vlan-id> | name <vlan_name>]
```

vlan_id	VLAN number
---------	-------------

vlan_name	VLAN name
-----------	-----------

If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Example:

```
P330-N# clear vlan 100
This command will assign all ports on vlan 100 to their
default in the entire management domain - do you want to
continue (Y/N)? y
VLAN 100 was deleted successfully
```

copy module-config scp

User level: supervisor

Use the `copy module-config scp` command to upload the switch-level parameters from the current NVRAM running configuration into a file via SCP.

The syntax for this command is:

```
copy module-config scp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the SCP server
mod-num	The switch number

Example:

```
P330-N# copy module-config scp c:\config\switch1.cfg 192.168.49.10 5
Username: 330user
Password:
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****
```

copy module-config tftp

User level: supervisor

Use the `copy module-config tftp` command to upload the switch-level parameters from the current NVRAM running configuration into a file via TFTP.

The syntax for this command is:

```
copy module-config tftp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the TFTP server
mod-num	The switch number

Example:

```
P330-N# copy module-config tftp c:\config\switch1.cfg 192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show tftp upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****
```

copy running-config scp

User level: supervisor

Use the **copy running-config scp** command to upload the current switch-level parameters from the current NVRAM running configuration into a file via SCP.

The syntax for this command is:

```
copy running-config scp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the SCP server
mod-num	The switch number

Example:

```
P330-N# copy running-config scp c:\config\switch1.cfg 192.168.49.10 5
Username: 330user
Password:
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy running-config startup-config

User level: supervisor

- ① This command applies to the P334T-ML only when it is in “Layer2” device mode.

Use the `copy running-config startup-config` command to copy the active policy configuration to the startup configuration file in the NVRAM.

The syntax for this command is:

copy running-config startup-config

Example:

```
P330-N# copy running-config startup-config
```

copy running-config tftp

User level: supervisor

- ① This command applies to the P334T-ML only when it is in “Layer2” device mode.

Use the `copy running-config tftp` command to upload the policy configuration to a TFTP server.

The syntax for this command is:

copy running-config tftp <filename> <ip>

filename Destination file name in the tftp server (full path).

ip The ip address of the tftp server.

Example (for Windows):

```
P330-N# copy running-config tftp c:\P330-ML\startup.cfg  
149.49.100.41
```

Example: (for Unix):

```
P330-N# copy running-config tftp /folder/P330-  
ML/startup.cfg 149.49.100.41
```

copy scp module-config*User level: supervisor*

Use the `copy scp module-config` command to download a module configuration to the device via SCP.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

copy scp module-config <filename> <ip>

filename Source file name on the SCP server (full path).

ip The ip address of the SCP server.

Example (for Windows):

```
P330-N# copy scp module-config c:\P330-ML\module.cfg 149.49.100.41
```

```
Username: 330user
```

```
Password:
```

```
Beginning download operation ...
```

```
This operation may take a few minutes...
```

```
Please refrain from any other operation during this time.
```

```
For more information , use 'show download status' command
```

```
*****
```

```
* If you are currently running the P330-ML Device Manager  
application,*
```

```
* it is recommended to exit from it before performing configuration*
```

```
* download operations. *
```

```
*****
```

Example: (for Unix):

```
P330-N# copy scp module-config /folder/P330-ML/module.cfg
149.49.100.41
Username: 330user
Password:
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show download status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy scp stack-config

User level: supervisor

Use the `copy scp stack-config` command to download a stack configuration to the device via SCP.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy scp stack-config <filename> <ip>
```

`filename` Source file name on the SCP server (full path).

`ip` The ip address of the SCP server.

Example (for Windows):

```
P330-N# copy scp stack-config c:\P330-ML\stack.cfg 149.49.100.41
Username: 330user
Password:
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show download status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

Example: (for Unix):

```
P330-N# copy scp stack-config /folder/P330-ML/stack.cfg 149.49.100.41
Username: 330user
Password:
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show download status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy scp startup-config*User level: supervisor*

Use the `copy scp startup-config` command to download a startup configuration to the device via SCP.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy scp startup-config <filename> <ip>
```

`filename` Source file name on the SCP server (full path).

`ip` The ip address of the SCP server.

Example (for Windows):

```
P330-N# copy scp startup-config c:\P330-ML\startup.cfg 149.49.100.41
Username: 330user
Password:
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show download status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

Example: (for Unix):

```
P330-N# copy scp startup-config /folder/P330-ML/startup.cfg
149.49.100.41
Username: 330user
Password:
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show download status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy stack-config scp

User level: supervisor

Use the `copy stack-config scp` command to upload the switch-level parameters from the active bank into a file via SCP.

The syntax for this command is:

```
copy stack-config scp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the SCP server
mod-num	The switch number

Example:

```

P330-N# copy stack-config scp c:\config\switch1.cfg 192.168.49.10 5
Username: 330user
Password:
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****

```

copy stack-config tftp*User level: supervisor*

Use the `copy stack-config tftp` command to upload the stack-level parameters from the current NVRAM running configuration into a file via TFTP.

- ① Create the file into which you wish to upload the stack-level parameters prior to executing this command.

The syntax for this command is:

```
copy stack-config tftp <filename> <ip>
```

filename	The file name (full path)
ip	The IP address of the TFTP server

Example:

```

P330-N# copy stack-config tftp c:\conf.cfg 192.168.49.10
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'upload status' command
*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****

```

copy startup-config scp*User level: supervisor*

Use the `copy startup-config scp` command to upload the switch-level startup configuration from the active bank into a file via SCP.

The syntax for this command is:

```
copy startup-config scp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the SCP server
mod-num	The switch number

Example:

```
P330-N# copy startup-config scp c:\config\switch1.cfg 192.168.49.10 5
Username: 330user
Password:
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy startup-config tftp*User level: supervisor*

- ① This command applies to the P334T-ML only when it is in “Layer2” device mode.

Use the `copy startup-config tftp` command to download a policy configuration from a TFTP server.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy startup-config tftp <filename> <ip>
```

filename Destination file name in the tftp server (full path).

ip The ip address of the tftp server.

Example (for Windows):

```
Router-N (super) # copy startup-config tftp c:\P330-ML\startup.cfg 149.49.100.41
```

Example: (for Unix):

```
Router-N (super) # copy startup-config tftp /folder/P330-ML/startup.cfg 149.49.100.41
```

copy tftp EW_archive

User level: supervisor

Use the `copy tftp EW-archive` command to download the P330-ML Manager application into the switch from a TFTP server.

The syntax for this command is:

```
copy tftp EW_archive <filename> <ip> <module number>
```

filename P330-ML Manager image file name (full path)

ip The IP address of the host

module number Module to download the embedded web to

Example (for Windows):

```
P330-N# copy tftp EW-archive c:\P330-ML\switch1.cfg 192.168.49.10 5
```

Example: (for Unix):

```
P330-N# copy tftp EW-archive /folder/startup.cfg 149.49.100.41 5
```

copy tftp module-config

User level: supervisor

Use the `copy tftp module-config` command to download the switch-level configuration from a saved file into the current NVRAM running configuration of a switch from a TFTP server.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy tftp module-config <filename> <ip>
```

filename	The file name (full path)
ip	The ip address of the TFTP server

Example (for Windows):

```
Router-N# copy tftp module-config c:\config\switch1.cfg  
192.168.49.10
```

Example: (for Unix):

```
Router-N# copy tftp module-config /folder/startup.cfg  
192.168.49.10
```

copy tftp stack-config

User level: supervisor

Use the `copy tftp stack-config` command to download the stack-level configuration from a saved file into the current NVRAM running configuration from a TFTP server.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy tftp stack-config <filename> <ip>
```

filename	The file name (full path)
ip	The IP address of the TFTP server

Example (for Windows):

```
Router-N# copy tftp stack-config c:\config\switch1.cfg  
192.168.49.10
```

Example (for Unix):

```
Router-N# copy tftp stack-config /folder/switch1.cfg  
192.168.49.10
```

copy tftp startup-config

User level: supervisor

① This command applies to the P334T-ML only when it is in “Layer2” device mode.

Use the `copy tftp startup-config` command to download a startup configuration from the saved TFTP file to the Startup Configuration file in the NVRAM.

① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy tftp startup-config <filename> <ip>
```

filename	Destination file name in the tftp server (full path)
ip	The ip address of the tftp server.

Example (for Windows):

```
Router-N (super) # copy tftp startup-config c:\P330-  
ML\startup.cfg 149.49.100.41
```

Example: (for Unix):

```
Router-N (super) # copy tftp startup-config  
/folder/startup.cfg 149.49.100.41
```

copy tftp SW_image

User level: supervisor

Use the `copy tftp SW_image` command to download a new firmware software version into bank B while either keeping the old version in bank A, or downloading the Embedded Web manager software into bank A.

The syntax for this command is:

```
copy tftp SW_image <sw_image_file> EW_archive <EmWeb_file>  
<IP_addr> <mod_num>
```

<code>sw_image_file</code>	Firmware image file name (full path)
<code>EmWeb_file</code>	Embedded Web Manager image file name (full path) - Optional, can be a dummy name
<code>IP_addr</code>	The ip address of the TFTP server
<code>mod_num</code>	Target switch module number

Example (for Windows):

```
P330-N# copy tftp SW_image c:\versions\P330-ML\p333t  
EW_image x 149.49.138.170 1
```

Example (for Unix):

```
P330-N# copy tftp SW_image /folder/versions/P330-ML/p333t  
EW_image x 149.49.138.170 1
```

- ① If file "x" does not exist, the Embedded web image will not be downloaded and bank A will retain the previous SW version image.

Example:

```
P330-N# copy tftp SW_image /home/P330-ML/viisa EW_archive 1  
135.64.103.104 1  
  
Module          : 1  
Source file     : /home/P330-ML/viisa  
Destination file : P330-ML  
Host           : 135.64.103.104  
Running state   : Download Process Started  
Failure display : no-error  
Last warning    : -  
.....  
Module          : 1  
Source file     : /home/P330-ML/viisa  
Destination file : P330-ML  
Host           : 135.64.103.104  
Running state   : Testing ...  
Failure display : no-error  
Last warning    : -  
.....  
Module          : 1  
Source file     : /home/P330-ML/viisa  
Destination file : P330-ML  
Host           : 135.64.103.104  
Running state   : Erasing FLASH  
Failure display : no-error  
Last warning    : -  
.....  
Module          : 1  
Source file     : /home/P330-ML/viisa  
Destination file : P330-ML  
Host           : 135.64.103.104  
Running state   : Downloading ...  
Failure display : no-error  
Last warning    : -  
...  
Module          : 1  
Source file     : /home/P330-ML/viisa  
Destination file : P330-ML  
Host           : 135.64.103.104  
Running state   : Download Ok  
Failure display : no-error  
Last warning    : -
```

copy tftp SW_powerinline_image*User level: supervisor*

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `copy tftp SW_powerinline_image` command to update the inline software application from a TFTP server to the memory of a designated module. You need to be in privilege mode to execute this command.

The syntax for this command is:

```
copy tftp SW_powerinline_image <image-file> <ip-addr> <mod-
num>
```

<code>image_file</code>	Common name for the file that contain the Power over Ethernet (PoE) Software image and the Embedded Web archive (full path)
<code>ip_addr</code>	IP address of the TFTP host
<code>mod_num</code>	Target module number

Example:

```
P330-ML-2# copy tftp SW_powerinline_image
c:\p333t\p333T_203 192.168.49.10 5
Module: 5
Source file: c:\p333t\p333t_203
Destination file: Powerinline
Host: 192.168.49.10
Running state: Downloading
Failure Display: Access Violation
Last warning:

Download completed
```

- ① Before executing the download, the following checks will be performed by embedded SW, on the TFTP server file:
 - Ensure that the file size is within its allocated space.
 - Check that the file contains embedded web SW for this application
 - Verify file validity by calculating the checksum.

crypto key generate dsa*User level: supervisor*

Use the `crypto key generate` command to create the host key.

The syntax for this command is:

```
crypto key generate dsa [key-size <key-length>]
```

key-size	A keyword specifying that the key length is provided by the user.
key-length	The number of bits in the key. Possible values are: 512 – 2048. The default is 768 bits.

Example:

```
P330-ML-2# crypto key generate dsa key-size 768
Generating DSA key, This command may take a few minutes...
.....
Key was created!
Key version: SSH2, DSA
Key Fingerprint:
a5:f8:4a:5d:c5:b5:9c:b5:26:51:2b:36:02:c0:18:a4
```

dir

User level: user, privileged, supervisor

Use the `dir` command to show the file types that have been downloaded to the switch.

The syntax for this command is:

```
dir [module_number]
```

Example:

```
P330-N>dir
M# file                ver num  file type  file location  file description
-- ----
1  Booter_Image         3.5.17   SW BootImage  Nv-Ram        Booter Image
1  module-config       N/A      Running Conf  Ram           Module Configuration
1  stack-config        N/A      Running Conf  Ram           Stack Configuration
1  EW_Archive          N/A      SW Web Image  Nv-Ram        Web Download
2  Booter_Image         3.2.5    SW BootImage  Nv-Ram        Booter Image
2  module-config       N/A      Running Conf  Ram           Module Configuration
2  EW_Archive          N/A      SW Web Image  Nv-Ram        Web Download
```

Output Fields:

Field	Description
M#	The switch number
file	There are several files loaded into the switch's memory: <ul style="list-style-type: none">• module-config – file which contains the configuration settings made to this switch• stack-config – file which contains the configuration settings made at the stack level (for example IP address of the stack)• EW_Archive – file which contains the Device Manager (Embedded Web) software• Booter_Image - file containing the booter code executed after rest. This file Can't be replaced by the user.• startup-config - file which contains the startup (saved in NVRAM) configuration for policy and routing in the P330-ML-ML, P333R, and P333R-LB• running-config - file which contains the running (currently active) configuration for policy and routing in the P330-ML-ML, P333R, and P333R-LB
ver num	S/W Version number – relevant only for Device Manager and Booter image.
file type	There are several file types: <ul style="list-style-type: none">• Running Conf – the configuration currently in use.• Startup-config - startup configuration for policy and routing in the P330-ML-ML, P333R, and P333R-LB• SW boot image - Booter file• SW Web Image – Device Manager S/W archive file
file location	Type of internal memory into which the file is loaded
file description	Description of the file

- ⓘ If N/A is displayed for the EW_Archive file, this means that the Device Manager software is not loaded correctly. Download the Device Manager software again.

disconnect ssh

User level: supervisor

Use the `disconnect ssh` command to disconnect an SSH session.

The syntax for this command is:

```
disconnect ssh <session-id>
```

session-id

The SSH session ID. Use the `show ssh` command to learn an SSH session ID.

Example:

```
P330-ML-2# disconnect ssh 0x508622f0

You are about to close this session - do you want to
continue (Y/N)? y

Closing session 0x508622f0
```

get time

User level: privileged, supervisor.

Use the `get time` command to retrieve the time from the network.

The syntax for this command is:

```
get time
```

Example:

```
P330-N>get time
Time is being acquired from server 0.0.0.0
Time has been acquired from the network.
```

help

User level: user, privileged, supervisor

Use the `help` command to print a list of all possible commands at the current level. If a command is specified and has no further sub-command(s), the help for that command is printed. If the command has a further sub-command, a brief description of the sub-command is printed.

The syntax for this command is:

```
help [<command> [<subcommand>...]]
```

Example:

```
P330-N>help username
Username commands:
-----
Usage: username <name> password <passwd> access-type {read-
only|read-write|admin}
```

hostname

User level: privileged, supervisor.

Use the `hostname` command to change the Command Line Interface (CLI) prompt. The current module number always appears at the end of the prompt.

Use the `no hostname` command to return the CLI prompt to its default.

The syntax for this command is:

```
[no] hostname [<hostname_string>]
```

- | | |
|-----------------|---|
| hostname_string | <ul style="list-style-type: none"> • none – displays current hostname • string – the string to be used as the hostname (up to 20 characters). |
|-----------------|---|

Examples:

```
P330-N# hostname
Session hostname is 'P330-ML'
```

```
P330-N# hostname "gregory"
gregory-N#
```

```
gregory-N# no hostname
P330-N#
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

ip access-list

User level: supervisor

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access list` command to create a specific policy rule. The access list

contains several of these rules: each rule pertains to the source IP address, the destination IP address, the protocol, the protocol ports (if relevant), and to the ACK bit (if relevant).

Use the `no ip access list` command to delete a specific rule.

The syntax for this command is:

```
[no] ip access-list <access-list-number> <access-list-index>
      <action> <protocol> {<source-ip>
      <source-wildcard> | any | host
      <source-ip>}<operator> <port> [<port>]
      {<destination-ip> <destination-
      wildcard>|any | host
      <destination-ip>}<operator> <port>
      [<port>]][established] [precedence]
```

<access-list-number>	integer (100...149)
<access-list-index>	integer (1...254)
<action>	permit deny deny-and-notify fwd0-7
<protocol>	ip tcp udp integer (1...255)
<source-ip>	ip address of the source network
<source-wildcard>	ip address wildcard of the source network
<operator>	eq lt gt range
<port>	integer (1...65535)
<destination-ip>	ip address of the destination network
<destination-wildcard>	ip address wildcard of the destination network
<precedence>	mandatory — rule is mandatory for this access list (an invalid rule invalidates entire list) optional — rule is optional for this access list (an invalid rule does not invalidate entire list)

Example:

```
Router-N# ip access-list 101 23 deny ip any
1.2.0.0 0.0.255.255
Router-N# ip access-list 101 24 fwd3 udp any host 10.1.1.1
range 20 23 optional
```

- ① The P334T-ML does not support 'lt' and 'gt' port operators.

ip access-list-cookie

User level: supervisor

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-cookie` command to set the list cookie for a specific policy list.

The syntax for this command is:

```
ip access-list-cookie <list-id> <cookie>
```

<list-id> integer (100...149, 0-default list)

<cookie> integer

Example:

```
Router-N# ip access-list-cookie 101 12345
```

ip access-list-copy

User level: supervisor

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-copy` command to copy a configured source policy list to a destination policy list.

The syntax for this command is:

```
ip access-list-copy <source-list> <destination-list>
```

<source-list> integer (100...149, 0-default list)

<destination-list> integer (100...149)

Example:

```
Router-N# ip access-list-copy 100 101
```

ip access-default-action*User level: supervisor*

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-default-action` command to set the default action for a specific policy list.

The syntax for this command is:

```
ip access-default-action <policy-list-number> <default-action>
```

<policy-list-number>	integer (100...149)
<default-action>	default-action-deny default-action-permit

Example:

```
Router-N# access-default-action 101 default-action-deny
Done!
```

ip access-list-dscp operation*User level: supervisor*

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-dscp operation` command to set a DSCP to CoS mapping. The system performs the mapping for only those frames than match an ACL rule with a 'permit' action.

The syntax for this command is:

```
ip access-list-dscp operation <policy-list-number> <dscp>
<action>
```

policy-list-number	A valid id number for a policy list currently defined for the module (100..149)
dscp	DSCP value or range of DSCP

- action permit | deny | deny-and-notify | fwd0 | fwd1... fwd7:
- permit: do nothing, let the packet pass
 - deny: drop the packet
 - deny-and-notify: drop the packet and send an SNMP trap
 - fwd0, fwd1...fwd7: set the frame COS field to 0...7

Example:

```
Router-N# ip access-list-dscp operation 101 0-63 permit
Router-N# ip access-list-dscp operation 101 62 fwd5
```

ip access-list-dscp trust

User level: supervisor

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-dscp trust` command to decide which original frame priority to trust for the placement of the frame in the internal priority queues.

The syntax for this command is:

```
ip access-list-dscp trust <policy-list-number>
{untrusted|trust-cos |trust-dscp }
```

- | | |
|--------------------|---|
| policy-list-number | A valid id number for a policy list currently defined for the module (100...149) |
| untrusted | Forward the packet with priority 0 |
| trust-cos | Forward the packet with its original 802.1p priority (default) |
| trust-dscp | Forward the packet with the maximum priority between 802.1p and the priority obtained from the DSCP-CoS mapping table |

Example:

```
Router-N# ip access-list-dscp trust 100 trust-dscp
Done!
```

ip access-list-name*User level: supervisor*

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-name` command to assign a name to a policy list.

The syntax for this command is:

```
ip access-list-name <policy-list-number> <name>
```

<policy-list-number> integer (100...149)

<name> list name

Example:

```
Router-N# ip access-list-name 101 morning
```

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

ip access-list-owner*User level: supervisor*

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip access-list-owner` command to set the owner for a specific policy list.

The syntax for this command is:

```
ip access-list-owner <policy-list-number> <owner>
```

<policy-list-number> integer (100...149)

<owner> list owner

Example:

```
Router-N# ip access-list-owner 101 admin  
Done!
```

ip http enable

User level: supervisor

Use the `ip http enable` command to enable HTTP access to the device.

The syntax for this command is:

ip http enable

Example:

```
P330-N# ip http enable
Done!
```

ip icmp redirect

User level: supervisor

Use the `ip icmp redirect` command to enable ICMP redirects via the device.

The syntax for this command is:

ip icmp redirect

Example:

```
P330-N# ip icmp redirect
Done!
```

ip simulate

User level: supervisor

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `ip simulate` command to check the policy for a simulated packet. The command contains the addressed list number, and the packet parameters.

The syntax for this command is:

```
ip simulate <policy-list-number> [<priority>] [<dscp-
value>]<source> <destination> [<protocol> [<source port>
<destination port> [<established>]]]
```

policy-list-number	integer (100...149, 0-default list)
priority	fwd0 fwd1 ... fwd7
dscp-value	dscp0 dscp1 ... dscp63

source	source ip address
destination	destination ip address
protocol	ip tcp udp integer (1...255)
source port	integer (1...65535)
destination port	integer (1...65535)
established	value of TCP established bit

Example:

```
Router-N(configure)# ip simulate 100 192.67.85.12  
193.76.54.25
```

ip ssh enable

User level: supervisor

Use the `ip ssh` command to enable the SSH server.

The syntax for this command is:

ip ssh enable

Example:

```
P330-N# ip ssh enable  
Done!
```

ip telnet enable

User level: supervisor

Use the `ip telnet enable` command to enable Telnet access to the device.

The syntax for this command is:

ip telnet enable

Example:

```
P330-N# ip telnet enable  
Done!
```

ip telnet-client enable

User level: supervisor

Use the `ip telnet-client enable` command to enable the device to act as a Telnet client.

① This command can only be run from the console port on the device.

The syntax for this command is:

ip telnet-client enable

Example:

```
P330-N# ip telnet-client enable
Done!
```

no ip http

User level: supervisor

Use the `no ip http` command to disable HTTP access to the device.

The syntax for this command is:

no ip http

Example:

```
P330-N# no ip http
Done!
```

no ip icmp redirect

User level: supervisor

Use the `no ip icmp redirect` command to disable ICMP redirects via the device.

The syntax for this command is:

no ip icmp redirect

Example:

```
P330-N# no ip icmp redirect
Done!
```

no ip ssh

User level: supervisor

Use the `no ip ssh` command to disable the SSH server.

The syntax for this command is:

no ip ssh

Example:

```
P330-N# no ip ssh
This will prevent future remote SSH sessions and disconnect
all active SSH sessions - do you want to continue (Y/N)? y
Shutting down all active sessions
```

no ip telnet

User level: supervisor

Use the `no ip telnet` command to disable Telnet access to the device.

The syntax for this command is:

no ip telnet

Example:

```
P330-N# no ip telnet
This will prevent future remote telnet sessions and
disconnect all active telnet sessions - do you want to
continue (Y/N)? y
Done!
```

no ip telnet-client

User level: supervisor

Use the `no ip telnet-client` command to disable the device from acting as a Telnet client.

① This command can only be run from the console port on the device.

The syntax for this command is:

no ip telnet-client

Example:

```
P330-N# no ip telnet-client  
Done!
```

no rmon alarm

User level: privileged, supervisor.

Use the `no rmon alarm` command to delete an existing RMON alarm entry.

The syntax for this command is:

```
no rmon alarm <Alarm Index>
```

Alarm Index	Alarm index defined using <code>rmon alarm</code> command or P330-ML Manager
-------------	--

Example:

```
P330-N# no rmon alarm 1026
```

no rmon event

User level: privileged, supervisor.

Use the `no rmon event` command to delete an existing RMON event entry.

The syntax for this command is:

```
no rmon event <Event Index>
```

Event Index	Event index defined using <code>rmon event</code> command or P330-ML Manager
-------------	--

```
P330-N# no rmon event 1054
```

no rmon history

User level: privileged, supervisor.

Use the `no rmon history` command to delete an existing RMON history entry.

The syntax for this command is:

```
no rmon history <History Index>
```

History Index	History index defined using <code>rmon history</code> command or RMON management tool
---------------	---

Example:

```
P330-N# no rmon history 1026
```

no snmp-server

User level: supervisor

Use the `no snmp-server` command to deny SNMP access to the device.

The syntax for this command is:

```
no snmp-server
```

Example:

```
P330-N# no snmp-server
Done!
```

no snmp-server engineID

User level: supervisor

Use the `no snmp-server engineID` command to return to the default SNMP engineID.

The syntax for this command is:

```
no snmp-server engineID
```

Example:

```
P330-N# no snmp-server engineID
EngineID return to default
Done!
```

no snmp-server community

User level: supervisor

Use the `no snmp-server community` command to deny access to the device using community strings.

The syntax for this command is:

no snmp-server community

Example:

```
P330-N# no snmp-server community
Done!
```

no snmp-server group

User level: supervisor

Use the `no snmp-server group` command to remove a specified SNMP group. When a security module is not provided, all instances of the group are removed. If a security model and level are specified, then only corresponding group instance is removed

The syntax for this command is:

no snmp-server group <groupname> {**v1** | **v2c** | **v3** {**noauth** | **auth** | **priv**}}

groupname	The name of the SNMP group.
v1, v2c, v3	The security model to remove from the group.
noauth, auth, priv	Keywords that specifies the type of authentication model instance to remove from the group. <ul style="list-style-type: none">• noauth• auth• priv

Example:

```
P330-1(super)# no snmp-server group newgroupG v3 noauth
Done!
```

no snmp-server host*User level: supervisor*

Use the `no snmp-server host` command to either delete the host from the trap recipients list or, if notifications types are specified in the command, disable the specified notifications for the host.

The syntax for this command is:

no snmp-server host <host-addr> [<notification-type-list>]

`host-addr` Specifies the address (or host name) of the notification recipient agent. The maximum length is 32 bytes.

`notification-type-list` List of notification types. Each types combines related notifications. You can disable notification generations on a per group basis. For example, the `swRedundancy` type groups new and delete software redundancy notifications.

(Optional)

If no `notification-type-list` is specified, the default, `all`, is used.

- `all/*` – All traps
- `generic` – Generic traps
- `config` – Config change notifications
- `eth-port-faults` – Ethernet port fault notifications
- `sw-redundancy` – Software redundancy notifications
- `temperature` – Temperature warning notifications
- `cam-change` – Changes in CAM notifications
- `l3-faults` – Layer 3 faults, including duplicate IP and VLAN violations
- `lag-event` – Link aggregation faults and configuration changes
- `policy` – Changes in policy notifications (for L3 devices)
- `link-down-faults` – ITC proprietary link down notifications
- `supply` – Power supply notifications (main and backup)
- `fan` – FAN faults notifications (main and backup)
- `cascade` – Cascade connection fault notifications.

Note that the list of notification names is proprietary to ITC.

Example:

```
P330-N>no snmp-server host 149.49.38.221  
Done!
```

no snmp-server notifications

User level: supervisor

Use the `no snmp-server notifications` command to disable all available SNMP notifications.

The syntax for this command is:

no snmp-server notifications

Example:

```
P330-N# no snmp-server notifications  
Done!
```

no snmp-server remote-user

User level: supervisor

Use the `no snmp-server remote-user` command to remove a remote user configured to receive SNMP notifications.

The syntax for this command is:

no snmp-server remote-user <username> <engine-id>

`username` Variable that specifies the name of the SNMP user. The maximum length is 32 bytes.

`engine-id` The SNMP engine ID of the remote host.

Example:

```
P330-1(super)# no snmp-server remote-user CharlieBrown  
1a:e9:00:00:01:95:31:8a:9d  
Done!
```

no snmp-server user

User level: supervisor

Use the `no snmp-server user` command to remove an SNMP user account.

The syntax for this command is:

```
no snmp-server user <username> { v1 | v2c | v3 }
```

username Variable that specifies the name of the SNMP user. The maximum length is 32 bytes.

v1, v2c, v3 The security model assigned to the user in user to group association.

Example:

```
P330-1(super)# no snmp-server user CharlieBrown v3
Done!
```

no snmp-server view

User level: supervisor

Use the `no snmp-server view` command to remove a view or remove OIDs from a view.

The syntax for this command is:

```
no snmp-server view <view-name> [<oid-tree>]
```

view-name Name of the view.

oid-tree Object identifier (OID) of the ASN.1 subtree to be removed from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4. To specify a subtree family, use the asterisk as a wildcard character. For example, 1.3.6.1.2.1.2.2.1.*.1 excludes access from all elements of the first row in IfTable. Symbolic MIB object names are not supported.

Example:

```
P330-N>no snmp-server view initial2
Done!
```

no username

User level: supervisor

Use the `no username` command to remove a local CLI user account.

The syntax for this command is:

```
no username <name>
```

name	User name
------	-----------

Example:

```
P330-1(super)# no username john
User account removed.
```

If you wish to delete a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

❶ You cannot delete the default user account “root”.

nvrn initialize

User level: privileged, supervisor.

Use the `nvrn initialize` command to reset the configuration parameters to their factory defaults.

The syntax for this command is:

```
nvrn initialize {switch | all}
```

switch	Resets all the switching parameters (Layer 2 only) throughout the stack
--------	---

all	Resets all parameters including licenses and routing parameters of the Layer 3 switches present in the stack
-----	--

Example:

```
P330-N# nvrn initialize
This command will restore factory defaults, and can
disconnect your telnet session
*** Reset *** - do you want to continue (Y/N)? y
Connection closed by foreign host
```

ping

User level: user, privileged, supervisor

Use the `ping` command to send ICMP echo request packets to another node on the network.

❶ You can use this command via the master switch only.

The syntax for this command is:

```
ping [host[number]]
```

- host Host IP address/Internet address of route destination. If missing, then the host IP address specified in the last ping command is used.
- number Number of packets to send. If missing, then the number specified in the last ping command is used. If the last number is not available, the default is 4.

Example: to ping the IP address 149.49.48.1 three times:

```
P330-N>ping 149.49.48.1 3

PING 149.49.48.1: 56 data bytes
64 bytes from 149.49.48.1: icmp_seq=0. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=1. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=2. time=0. ms

----149.49.48.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

prompt-length

User level: supervisor

Use the `prompt-length` command to specify the length of the default CLI prompt.

The syntax for this command is:

```
prompt-length <full|<prompt-size>>
```

- full Display the full length of the prompt
- prompt-size Set the length in characters of the prompt to display

Example:

```
P330-ML-1(super)# prompt-length 4
~r)#
```

reset

User level: user, privileged, supervisor

Use the `reset` command to restart the stack or an individual switch. If no switch number is defined or the switch number of the Master is defined, the command resets the entire stack. If the switch number is defined, the command resets the specified switch only.

The syntax for this command is:

reset {module number}

Example:

To reset the Master agent and force the entire stack to reset:

```
P330-N# reset
This command will force a switch-over to the master module
and disconnect your telnet session.
Do you want to continue (y/n) [n]? y
Connection closed by foreign host.
```

To reset switch 4:

```
P330-N# reset 4
This command will reset module 4 and may disconnect your
telnet session.
Do you want to continue (y/n) [n]? y
Resetting module 4...
```

reset mgp

User level: privileged, supervisor.

Use the `reset mgp` command to perform a software reset in the G700 Media Gateway Processor.

The syntax for this command is:

reset mgp [module]

module Module number of the MGP

Example:

```
P330-N# reset mgp 1
```

reset stack

User level: privileged, supervisor.

Use the `reset stack` command to perform a hardware reset of the entire stack.

The syntax for this command is:

reset stack

reset wan

User level: user, privileged, supervisor

Use the `reset wan` command to perform a software reset in the X330 WAN Access Router Module.

The syntax for this command is:

`reset wan [module] [bank-a]`

To reset a WAN module residing on switch 2:

`module` Optional - the module number where the WAN module to be reset resides.

`bank-a` Optional - boot the WAN module from bank-a after reset.

retstatus

User level: supervisor

Use the `retstatus` to display the return status of the previously executed command.

The syntax for this command is:

`retstatus`

Example:

```
P330-N# retstatus
Succeeded
```

rmon alarm

User level: privileged, supervisor.

Use the `rmon alarm` command to create a new RMON alarm entry.

The syntax for this command is:

```
rmon alarm <Alarm Number> <variable> <interval> <sample type>
rising-threshold <rising threshold> <rising event> falling-
threshold <falling threshold> <falling event> <startup alarm>
<owner>
```

Alarm Number	This is the alarm index number of this entry (it is advisable to use the same interface number as your alarm index number.)
variable	The instance of an RMON statistic.
interval	The interval between 2 samples.
sample type	This can be set to either delta (the difference between 2 samples) or an absolute value.
rising threshold	This sets the upper threshold for the alarm entry.
rising event	The RMON event entry that will be notified if the upper threshold is passed.
falling threshold	This sets the lower threshold for the alarm entry.
falling event	The RMON event entry that will be notified if the lower threshold is passed.
startup alarm	The instances in which the alarm will be activated. The possible parameters are: Rising, Falling, risingOrfalling .
owner	Owner name string.

Example:

```
P330-N# rmon alarm 1026 1.3.6.1.2.1.16.1.1.1.5.1026 60
delta rising-threshold 10000 1054 falling-threshold 10 1054
risingOrFalling gregory
alarm 1026 was created successfully
```

rmon event

User level: privileged, supervisor.

Use the `rmon event` command to create an RMON event entry.

The syntax for this command is:

```
rmon event <Event Number> <type> description <description>
owner <owner>
```

event number	This is the event index number of this entry.
type	The type of the event. The possible parameters are: <ul style="list-style-type: none"> • trap • log • logAndTrap • none
description	A user description of this event
owner	Owner name string

Example:

```
P330-N# rmon event 1054 logAndTrap description "event for
monitoring gregory's computer" owner gregory
event 1054 was created successfully
```

rmon history

User level: privileged, supervisor.

Use the `rmon history` command to create an RMON history entry.

The syntax for this command is:

```
rmon history <history index> [<module>[</port>]] interval
<interval> buckets <number of buckets> owner <owner name>
```

history_index	History index number of this entry (it is advisable to use the same interface number as your history index number).
module/port	The switch number/the port number.
interval	The interval between 2 samples.
number of buckets	The number of buckets defined.

owner name The owner name string.

Example:

```
P330-N# rmon history 1026 1026 3/2 30 buckets 20 owner amir
history 1026 was created successfully
```

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

session

User level: user, privileged, supervisor

Use the `session` command to open a session with a specific entity within a switch or the stack. For example, you can open a session with the Routing entity of a P330-ML-ML switch in the stack, or with an the X330 ATM (or X330 WAN) sub-module entity plugged into a specific switch.

- ❶ Layer 2 commands are only available if you open a `switch` session with the Master switch.
- ❶ When you use the `session` command the security level stays the same.

The syntax for this command is:

```
session [<module_number> [switch|router|atm|mgp|wan]]
```

module_number	(optional) The switch number. If you do not specify this parameter, you will get the list of modules within the stack.
switch router atm mgp wan	(optional) The entity to which you want to open a session. If you do not specify this parameter, you will get the default entity of the specific module: switch - Layer 2 entity of the switch (see Note below). router - Routing entity. atm - ATM entity. mgp - Media Gateway Processor. wan - WAN access router entity.

Use the `session` command without any parameters to identify the stack master and its slot number. It will list all the modules in the stack and their slot number with the master module marked with an asterisk.

Example:

```
P330-1# session 2
P330-2# session
P333T (*) In Slot 1
P334T      In Slot 2
P330-2#
```

set allowed managers

User level: privileged, supervisor.

Use the `set allowed managers` command to enable or disable the Allowed Managers feature.

When this feature is enabled, only those stations whose IP addresses are listed in the Allowed Managers table can access the device over Telnet, SNMP, or HTTP.

The syntax for this command is:

```
set allowed managers [enabled|disabled]
```

Example:

```
P330-1(super)# set allowed managers enabled
Managers are enabled
```

set allowed managers ip

User level: privileged, supervisor.

Use the `set allowed manager ip` command to add or remove an IP address from the Allowed Managers table. The Allowed Managers table can contain up to twenty IP addresses.

The syntax for this command is:

```
set allowed managers ip [add | delete][IP address]
```

add	Adds specified IP address to the Allowed Managers table
delete	Deletes specified IP address from the Allowed Managers table
IP address	IP address to be added or removed

Example:

```
P330-N# set allowed managers ip add 149.49.32.134  
Ip was added to the table
```

set arp-aging-interval

User level: privileged, supervisor.

Use the `set arp-aging interval` command to set the ARP table aging interval for entries in the agent Layer 2 ARP table.

The entry is deleted at the end of every aging interval. The default value is 10 minutes.

The syntax for this command is:

```
set arp-aging-interval <value>
```

value	The number representing the interval, from 0-10 minutes. 0 - arp-aging interval is 20 minutes.
-------	--

Example:

```
P330-N# set arp-aging-interval 10  
ARP table aging interval was set to 10 minutes.
```

set arp-tx-interval

User level: privileged, supervisor.

Use the `set arp-tx-interval` command to set the keep-alive frames sending interval. The keep-alive frames in ARP packets for the P330-ML agent are used to ensure connectivity with the P330-ML agent is always achieved.

The syntax for this command is:

```
set arp-tx-interval <value>
```

value	The interval in seconds. (0-3600) 0 disables the transmission of the keep-alive frames.
-------	--

Example:

```
P330-N# set arp-tx-interval 15  
ARP tx interval was set to 15 seconds.
```

set autopartition

User level: privileged, supervisor.

- ① This command is not relevant to P330-ML-ML switches. It appears in the P330-ML-ML CLI for controlling autopartition of other P330-ML switches in the stack.

Use the `set autopartition` command to enable or disable auto-partitioning on P330-ML switches in the stack.

The syntax for this command is:

```
set autopartition <value> [module]
```

value	enable/disable
module	module slot number

Example:

```
P330-N# set autopartition enable 3
Auto-partition is enabled in module 3.
```

set boot bank

User level: privileged, supervisor.

- ① This command is not available on the P333R and P333R-LB.

Use the `set boot bank` command to configure the software bank from which the switch will boot at the next boot process. This command should be issued separately for each switch in the stack using the `session` command first.

- ① If you wish to execute this command on a switch other than the stack master, you must open a session the relevant switch.

The syntax for this command is:

```
set boot bank <value>
```

value	{bank-a bank-b}
-------	-------------------

Example:

```
P330-N# set boot bank bank-a
Boot bank is set to bank-a
```

set cascading

User level: privileged, supervisor.

Use the `set cascading` command to control the generation of fault-traps for unconnected cascading links. This command is useful when cascading cables are not connected intentionally, and therefore no fault-traps are desired for this event.

The syntax for this command is:

```
set cascading{up|down}fault-monitoring {enable|disable}  
<mod-num>
```

Example:

```
P330-N# set cascading down fault-monitoring enable 1  
Module 1 cascading-down fault monitoring enabled
```

set device-mode

User level: privileged, supervisor.

Use the `set device-mode` command to select the module's operating mode — Layer 2 or Router .

① This command is available on P330-ML-ML and P333R switches only.

The syntax for this command is:

```
set device-mode <mode>
```

- | | |
|------|---|
| mode | • Router – switch operates at Layers 2 and 3. |
| | • Layer2 – switch operates at Layer 2. |

Example:

```
Router-N# set device-mode Router  
This command will RESET the switch****  
Reset **** do you want to continue (Y/N) ?  
  
Done!
```

set dot1x max-req

User level: supervisor

Use the `set dot1x max-req` command to set maximum number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated.

The syntax for this command is:

```
P330-N> set dot1x max-req <count>  
count      Number of attempts – 1 to 10
```

Example:

```
P330-1 (super) # set dot1x max-req 3
```

set dot1x quiet-period

User level: supervisor

Use the `set dot1x quiet-period` command to set the minimal time between authentication attempts.

The syntax for this command is:

```
set dot1x quiet-period <Seconds>  
Seconds      Number of seconds – 0 to 65535
```

Example:

```
P330-1 (super) # set dot1x quiet-period 90  
Done!
```

set dot1x re-authperiod

User level: supervisor

Use the `set dot1x re-authperiod` command to set the idle time between re-authentication attempts.

The syntax for this command is:

```
set dot1x re-authperiod <Seconds>  
Seconds      Number of seconds – 0 to 65535
```

Example:

```
P330-1 (super) # set dot1x re-authperiod 90  
Done!
```

set dot1x server-timeout

User level: supervisor

Use the `set dot1x server-timeout` command to set the server retransmission timeout period for all ports. This is the maximum time that the port will wait for a reply from the Authentication Server.

The syntax for this command is:

```
set dot1x server-timeout <Seconds>
```

Seconds Number of seconds – 0 to 65535

Example:

```
P330-1(super)# set dot1x server-timeout 90
```

set dot1x supp-timeout

User level: supervisor

Use the `set dot1x supp-timeout` command to set the maximum time that the switch will wait for a reply from the Authenticated Station before the session is terminated.

The syntax for this command is:

```
set dot1x supp-timeout <Seconds>
```

Seconds Number of seconds – 0 to 65535

Example:

```
P330-1(super)# set dot1x supp-timeout 90
```

set dot1x system-auth-control disable

User level: supervisor

Use the `set dot1x system-auth-control disable` command to globally disable the PBNAC (802.1x) feature.

The syntax for this command is:

```
set dot1x system-auth-control disable
```

Example:

```
P330-1(super)# set dot1x system-auth-control disable  
dot1x system-auth-control disabled
```

set dot1x system-auth-control enable*User level: supervisor*

Use the `set dot1x system-auth-control enable` command to globally enable the PBNAC (802.1x) feature.

The syntax for this command is:

```
set dot1x system-auth-control enable
```

Examples:

- When a RADIUS server is defined:

```
P330-1(super)# set dot1x system-auth-control enable
dot1x system-auth-control enabled
```

- When a RADIUS server is not defined:

```
P330-1(super)# set dot1x system-auth-control enable
*** Warning : Authentication server ( RADIUS ) is
disabled/not-exist and so,
*** no authentication can be made
dot1x system-auth-control enabled
```

set dot1x tx-period*User level: supervisor*

Use the `set dot1x tx-period` command to set the time interval between attempts to access the Authenticated Station.

The syntax for this command is:

```
set dot1x tx-period <Seconds>
```

Seconds Number of seconds – 0 to 65535

Example:

```
P330-1 (super) # set dot1x tx-period 90  
Done!
```

set inband vlan

User level: privileged, supervisor.

Use the `set inband vlan` command to set the inband management VLAN.

The syntax for this command is:

```
set inband vlan <value>
```

value	Number of the VLAN to be assigned to the management interface.
-------	--

Example:

```
P330-N# set inband vlan 1  
Management VLAN number set to 1
```

set intelligent-multicast

User level: privileged, supervisor.

Use the `set intelligent-multicast` command to enable or disable the IP-multicast filtering application.

The syntax for this command is:

```
set intelligent-multicast {enable|disable}
```

Example:

```
P330-N# set intelligent-multicast enable  
Done!
```

set intelligent-multicast client-port-pruning time

User level: privileged, supervisor.

Use the `set intelligent-multicast client port pruning time` command to set the aging time for client ports. This is the time after the P330-ML switch reset during which the filtering information is learned by the switch but not configured on the ports.

The syntax for this command is:

```
set intelligent-multicast client-port-pruning time <seconds>  
  
seconds          Client port pruning time in seconds
```

Example:

```
P330-N# set intelligent-multicast client-port-pruning-time  
40  
Done!
```

set intelligent-multicast group-filtering-delay time

User level: privileged, supervisor.

Use the `set intelligent-multicast group-filtering delay time` command to set group filtering time delays. This is the time that the switch waits between becoming aware of a Multicast group on a certain VLAN and starting to filter traffic for this group.

The syntax for this command is:

```
set intelligent-multicast group-filtering-delay time <seconds>  
  
seconds          Group filtering time in seconds.
```

Example:

```
P330-N# set intelligent-multicast group-filtering-delay time  
40  
Done!
```

set intelligent-multicast router-port-pruning time

User level: privileged, supervisor.

Use the `set intelligent-multicast router-port-pruning time` command to set the aging time for router ports. This is a timer that ages out Router port information if IGMP queries are not received within the configured time.

The syntax for this command is:

```
set intelligent-multicast router-port-pruning time <seconds>  
  
seconds          Router port pruning time in seconds.
```

Example:

```
P330-N# set intelligent-multicast router-port-pruning-time  
40  
Done!
```

set interface inband

User level: privileged, supervisor.

Use the `set interface inband` command to configure the Management inband interface on the Master agent in the stack.

The syntax for this command is:

```
set interface inband <vlan> <ip_addr> <netmask>
```

`vlan` The number of the VLAN to be assigned to the interface

`ip_addr` IP address of the inband interface

`netmask` Subnet mask

Example:

To configure the inband interface on VLAN 1, IP address 1.1.1.1 and netmask 255.255.255.24:

```
P330-N# set interface inband 1 1.1.1.1 255.255.255.24  
Interface inband IP address set.  
You must reset the device in order for the change to take  
effect.
```

set interface ppp

User level: privileged, supervisor.

Use the `set interface ppp` command to configure the Master agent PPP interface IP parameters, exit modem mode, disconnect the PPP session, or reset the connected modem.

You must configure an IP address and net-mask for the P330-ML before you can establish a PPP connection. The IP address is a dummy address that is shared between two peers, and must be taken from a subnet that is different from the agent's inband IP subnet.

The syntax for this command is:

```
set interface ppp <ip_addr> <net-mask>
```

ip_addr	IP address used by the P330-ML Supervisor Module to connect via its PPP interface
net-mask	Subnet mask used by the P330-ML Supervisor Module to connect via its PPP interface

Example:

```
P330-N# set interface ppp 149.49.34.125 24
Interface ppp ip address set
```

set interface ppp enable/enable-always/disable/off/reset

User level: privileged, supervisor.

Use the `set interface ppp` command to enter modem mode, enter terminal mode, disconnect the PPP session or to reset the connected modem.

The syntax for this command is:

```
set interface ppp {enable|enable-always|disable|off|reset}
```

enable	Enable PPP and enter modem mode.
enable-always	Enter modem mode every time that the proprietary modem cable is plugged into the console port.
disable	Disable PPP and enter terminal mode
off	Disconnect the active PPP session.
reset	Reset the connected modem.

Example:

```
P330-N# set interface ppp reset
PPP has reset the connected modem.
```

Example:

```
P330-N# set interface ppp enable  
Entering the Modem mode within 60 seconds...  
Please check that the proprietary modem cable is plugged  
into the console port
```

Example:

```
P330-N# set interface ppp disable  
Entering the Terminal mode immediately
```

set intermodule port redundancy

User level: privileged, supervisor.

Use the `set intermodule port redundancy` command to define the stack's unique intermodule redundancy scheme. The defined scheme can be cleared using the `set intermodule port redundancy off` command.

- ① You must disable Spanning Tree before you can enable intermodule port redundancy.

The syntax for this command is:

```
set intermodule port redundancy <module/prim-port>  
<module/second-port> {on [<name>]}
```

<code>module/prim-port</code>	Primary port number
<code>module/second-port</code>	Secondary port number
<code>on</code>	Set the intermodule redundancy
<code>name</code>	Name of the fast redundancy (default is 'intermodule')

Example:

```
P330-N# set intermodule port redundancy 1/7 2/12 on  
backbone  
backbone: port 2/12 is intermodule redundant to port 1/7
```

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, e.g. "new york".

set intermodule port redundancy off

Use the `set intermodule port redundancy off` command to clear the intermodule port redundancy scheme.

The syntax for this command is:

```
set intermodule port redundancy off
```

Example:

```
P330-N# set intermodule port redundancy off
Intermodule port redundancy entry deleted.
```

set internal buffering

User level: privileged, supervisor.

- ① This command is not relevant to P330-ML-ML switches. It appears in the P330-ML-ML CLI for controlling internal buffering of other P330-ML switches in the stack.

The `set internal buffering` command allows you to set the size (Maximum, Medium, and Minimum) of the Receive (Rx) buffer allocated to each port of the specified switch. This command is meaningless when any port of the switch is operating with flow control ON.

The syntax for this command is:

```
set internal buffering <module> {value}
```

`module` Module number in the stack

`value` `max` - sets the internal receive buffer to its maximum size
 `med` - sets the internal receive buffer capacity dynamically
 `min` - sets the internal receive buffer to its minimum size
 Default is `min`

Example:

```
P330-N# set internal buffering 1 max
Done.
```

set ip route

User level: privileged, supervisor.

Use the `set ip route` command to add a route to the IP routing table. You can configure from 1 to 10 default static gateways for a P330-ML switch.

The syntax for this command is:

```
set ip route <destination> <gateway>
```

destination IP address of the network, or specific host to be added

gateway IP address of the router

Example:

This example shows how to add a default route to the IP routing table:

```
P330-N# set ip route 0.0.0.0 192.168.1.1
destination = 0.0.0.0 gateway = 192.168.1.1

ROUTE NET TABLE
destination      gateway          flags  Refcnt  Use      Interface
-----
0.0.0.0          192.168.1.1    1      1       3199     se0
127.1.1.0        127.1.1.1      1      8       7606     se1
-----

ROUTE HOST TABLE
destination      gateway          flags  Refcnt  Use      Interface
-----
127.0.0.1        127.0.0.1      5      2       131      lo0
10.10.10.10      192.168.1.1    7      0       0        se0
-----
```

set license

User level: privileged, supervisor.

Use the `set license` command to activate the SMON and Routing capabilities of the Avaya P330-ML stack. An Avaya P330-ML stack can include several Avaya P330-ML switches. One SMON license is required per Avaya P330-ML stack; a routing license is required for each P330-ML-ML switch in the stack.

For a full description of the SMON or Routing License and the installation procedure please refer to the Installation Guide provided with the SMON/Routing License.

The syntax for this command is:

```
set license [module] [license] [feature name]
```

module	Switch number
license	License number
feature name	Name of the feature, either smon or routing

Example:

```
P330-N# set license 1 021 1ad bad ca5 8d2 ccd smon
```

set logging file condition

User level: privileged, supervisor.

Use the `set logging file condition` command to define a filter rule for logging messages to the logging file.

The syntax for this command is:

```
set logging file condition { all | <application> } { none | <severity> }
```

all	A keyword signifying that messages from all applications are displayed.
-----	---

application	<p>The application from which logging messages are logged to the logging file. Possible values are:</p> <ul style="list-style-type: none">• BOOT• SYSTEM• ROUTER• CONFIG• FILESYS• FAN• SUPPLY• SECURITY• CASCADE• QOS• SWITCHFABRIC• LAG• VLAN• SNMP• POLICY• CLI• STP• THRESHOLD• CONSOLE
none	<p>A keyword signifying that logging messages are not logged to the logging file regardless of the severity of the message.</p>
severity	<p>The minimum severity of the logging messages that are logged to the logging file. Possible values are:</p> <ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notification• Informational• Debugging

Example:

```
P330-N# set logging file condition RIP Debugging  
Done!
```

set logging file disable

User level: privileged, supervisor.

Use the `set logging file disable` command to disable logging messages to a logging file.

The syntax for this command is:

```
set logging file disable
```

Example:

```
P330-N# set logging file disable  
Done!
```

set logging file enable

User level: privileged, supervisor.

Use the `set logging file enable` command to enable logging messages to a logging file.

The syntax for this command is:

```
set logging file enable
```

Example:

```
P330-N# set logging file enable  
Done!
```

set logging server

User level: privileged, supervisor.

Use the `set logging server` command to define the IP address of a logging server. You may define up to three logging servers.

```
set logging server <ip-address>
```

`ip-address` The IP address of the Syslog server.

Example:

```
P330-N# set logging server 149.49.38.22  
Done!
```

set logging server access-level

User level: privileged, supervisor.

Use the `set logging server access-level` command to define the access level associated with Syslog server sink. The user cannot specify an access level higher than the level assigned to him.

- ① You need to define a logging server using the `set logging server` command before you can set the server access level.

The syntax for this command is:

```
set logging server access-level < admission-level >  
<ip-address>
```

admission-level	The access level associated with the Syslog server sink. Possible values are: <ul style="list-style-type: none">• read-only• read-write• admin
ip-address	The IP address of the Syslog server.

Example:

```
P330-N# set logging server access-level read-only  
149.49.38.22  
Done!
```

set logging server condition

User level: privileged, supervisor.

Use the `set logging server condition` command to define a filter rule for logging messages to the Syslog server.

- ① You need to define a logging server using the `set logging server` command before you can set the server condition.

The syntax for this command is:

```
set logging server condition { all | <application> } { none | <severity> } <ip-address>
```

all	A keyword signifying that the specified severity threshold applies to all applications.
application	The application to which the filter applies. Possible values are: <ul style="list-style-type: none"> • BOOT • SYSTEM • ROUTER • CONFIG • FILESYS • FAN • SUPPLY • SECURITY • CASCADE • QOS • SWITCHFABRIC • LAG • VLAN • SNMP • POLICY • CLI • STP • THRESHOLD • CONSOLE
none	A keyword signifying that logging messages are not logged to the Syslog server regardless of the severity of the message.
severity	The minimum severity of the logging messages that are logged to the Syslog server. Possible values are: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
ip-address	The IP address of the Syslog server.

Example:

```
P330-N# set logging server condition LAG Warning  
135.64.102.224  
Done!
```

set logging server disable

User level: privileged, supervisor.

Use the `set logging server disable` command to disable logging messages to a Syslog server.

- ① You need to define a logging server using the `set logging server` command before you can disable the server.

The syntax for this command is:

```
set logging server disable <ip-address>
```

`ip-address` The IP address of the Syslog server.

Example:

```
P330-N# set logging server disable 149.49.35.21  
Done!
```

set logging server enable

User level: privileged, supervisor.

- ① Use the `set logging server enable` command to enable logging messages to a Syslog server.
- ① You need to define a logging server using the `set logging server` command before you can enable the server.

The syntax for this command is:

```
set logging server enable <ip-address>
```

`ip-address` The IP address of the Syslog server.

Example:

```
P330-N# set logging server enable 149.49.35.21
Done!
```

set logging server facility

User level: privileged, supervisor.

Use the `set logging server facility` command to update the server facility used for sending messages to Syslog server. Facility settings are done on per Syslog server.

- ① You need to define a logging server using the `set logging server` command before you can set the server facility.

The syntax for this command is:

```
set logging server facility <server-facility> <ip-address>
```

server-facility The facility used for sending messages to the Syslog server.

Possible values are:

- **kern** – Kernel
- **user** – User processes
- **mail** – Electronic mail
- **daemon** – Background system processes
- **auth** – Authorization
- **syslog** – System logger
- **lpr** – Printer
- **news** – Usenet news
- **uucp** – Unix-to-Unix copy program
- **clkd** – Clock daemon
- **sec** – Security
- **ftpd** – FTP daemon
- **ntp** – NTP subsystem
- **audi** – Log audit
- **alert** – Log alert
- **clkd2** – Clock daemon
- **local0-local7** – Available for user defined facilities

ip-address The IP address of the Syslog server.

Example:

```
P330-N# set logging server facility news 135.64.102.224  
Done!
```

set logging session condition

User level: privileged, supervisor.

Use the `set logging session condition` command to define a filter rule for logging messages during the current session.

The syntax for this command is:

```
set logging session condition { all | <application> } { none |  
<severity> }
```

<code>all</code>	A keyword signifying that the specified severity threshold applies to all applications.
<code>application</code>	The application to which the filter applies. Possible values are: <ul style="list-style-type: none">• BOOT• SYSTEM• ROUTER• CONFIG• FILESYS• FAN• SUPPLY• SECURITY• CASCADE• QOS• SWITCHFABRIC• LAG• VLAN• SNMP• POLICY• CLI• STP• THRESHOLD• CONSOLE
<code>none</code>	A keyword signifying that messages are not logged regardless of their severity.

severity The minimum severity of the logging messages that are logged.
Possible values are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notification
- Informational
- Debugging

Example:

```
P330-N# set logging session condition LAG Error  
Done!
```

set logging session disable

User level: privileged, supervisor.

Use the `set logging session disable` command to disable logging messages in the current CLI session.

The syntax for this command is:

set logging session disable

Example:

```
P330-N# set logging session disable  
Done!
```

set logging session enable

User level: privileged, supervisor.

Use the `set logging session enable` command to enable logging messages in the current CLI session.

The syntax for this command is:

set logging session enable

Example:

```
P330-N# set logging session enable  
Done!
```

set logout

User level: privileged, supervisor.

Use the `set logout` command to set the time in minutes before the system automatically disconnects an idle session.

The syntax for this command is:

```
set logout [timeout in minutes]
```

timeout in minutes	Time until the system automatically disconnects an idle session.
--------------------	--

- Setting the value to 0 disables the automatic disconnection of idle sessions
- Default value is 15 minutes

Examples:

- To set the time until the system disconnects an idle session automatically to 20 minutes:

```
P330-N# set logout 20  
Sessions will be automatically logged out after 20 minutes  
of idle time.
```

- To disable the automatic disconnection of idle sessions:

```
P330-N# set logout 0  
Sessions will not be automatically logged out.
```

set mac-aging

User level: privileged, supervisor.

① This command is available on the P330-ML-ML switches only.

Use the `set mac-aging` command to enable or disable the MAC aging function.

The syntax for this command is:

```
Set mac-aging <status>
```

```
status      enable / disable
```

Examples:

```
P330-N# set mac-aging enable
mac aging is enabled.
```

```
P330-N# set mac-aging disable
mac aging is disabled.
```

set mac-aging-time

User level: privileged, supervisor.

① This command is available on the P330-ML-ML switches only.

Use the `set mac-aging-time` command to set the MAC aging time in minutes. This is the time after which unused MAC addresses in the MAC table are erased.

The syntax for this command is:

```
Set mac-aging-time <aging-time>
```

```
aging-      Aging time in minutes (1-3600; default =5).
time
```

Example:

```
P330-N# set mac-aging-time 5
mac aging time is set to 5 minutes.
```

① The entered value is the aging time lower limit. The actual aging time might be up to three minutes longer.

set port auto-negotiation-flowcontrol-advertisement

User level: privileged, supervisor.

Use the `set port auto-negotiation-flowcontrol-advertisement` command to set the flowcontrol advertisement for a Gigabit port when performing autonegotiation.

The syntax for this command is:

```
set port auto-negotiation-flowcontrol-advertisement
```

```
<module>/<port> {no-flowcontrol | asym-tx-only | sym-only | sym-and-  
asym-rx}
```

module	Number of the module.
port	Number of the port on the module. If you do not specify a number, all the ports on the module are set. Alternatively, you can specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.
no-flowcontrol	The port will advertise no pause capabilities.
asym-tx-only	The port will advertise asymmetric Tx pause capabilities only.
sym-only	The port will advertise symmetric pause capabilities only.
sym-and-asym-rx	The port will advertise both symmetric and asymmetric Rx pause capabilities.

Example:

```
P330-N# set port auto-negotiation-flowcontrol-  
advertisement 1/5 asym-tx-only
```

```
Port 1/5 pause capabilities was set
```

set port channel

User level: privileged, supervisor.

Use the `set port channel` command to enable or disable a Link Aggregation Group (LAG) interface on the switch. LAG creation requires a LAG name to be specified. There is no default name.

You can also add or remove a port from an existing LAG. When adding or removing a port to an existing LAG, type the same LAG-name. All ports in the LAG are configured with the parameters of the first port that is added to the LAG. These parameters include port administrative status, speed, duplex, autonegotiation mode, VLAN ID, tagging mode, binding mode, and priority level.

The ports added to a LAG must belong to the same LAG group - refer to the “LAG” marking on device’s front panel.

- ❶ When adding a port to an existing LAG, type the same LAG name, otherwise you will create a new LAG.

The syntax for this command is:

```
set port channel [<port_list>] [<value>] [<name>]
```

port_list	A list of ports to be aggregated in the format module/port
value	on or off – enables or disables the channel for the specified module ports
name	Channel name

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

Example:

```
P330-N# set port channel 1/5-6,8 on my-channel
Port 1/5 channel mode set to on 1/102
Port 1/6 was added to channel 1/102
Port 1/8 was added to channel 1/102
```

set port classification

User level: privileged, supervisor.

Use the `set port classification` command to set the port classification to either regular or valuable. Any change in the Spanning Tree state from Forwarding for a valuable port will erase all learnt MAC addresses in the stack.

The syntax for this command is:

```
set port classification [module/port] {regular|valuable}
```

module port	module/port range
regular valuable	port classification

Example:

```
P330-N# set port classification 2/19 valuable
Port 2/19 classification has been changed.
```

set port disable

User level: privileged, supervisor.

Use the `set port disable` command to disable a port or range of ports.

The syntax for this command is:

```
set port disable <mod_num>/<port_num>
```

module	Number of the switch in the stack.
port	Number of the port on the module. If you do not specify a number, all the ports on the module are disabled. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example:

```
P330-N# set port disable 4/1  
  
Port 4/1 disabled.
```

set port dot1x initialize

User level: supervisor

Use the `set port dot1x initialize` command to initialize port dot1x.

The syntax for this command is:

```
set port dot1x initialize <module/port>
```

module/	Module and port number
port	You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example:

```
P330-1(super)# set port dot1x initialize 2/3  
  
port 1/2 dot1x was initialized
```

set port dot1x max-req

User level: supervisor

Use the `set port dot1x max-req` command to set the maximal number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated.

The syntax for this command is:

```
set port dot1x max-req <module/port> <count>
```

module/ Module and port number (or range of ports)

port

count Number of attempts — 1-10

Example:

```
P330-N>set port dot1x max-req 1/2 5
```

set port dot1x port-control

User level: supervisor

Use the `set port dot1x port-control` command to set the dot1x parameter per port.

The syntax for this command is:

```
set port dot1x port-control <module/port> <mode>
```

module/ Module and port number (or range of ports)

port

mode force-unauthorize - the port is always is blocking state
 auto - forwarding/blocking depends on authorization outcome
 force-authorize - the port is always in forwarding state

Example:

```
P330-1(super)# set port dot1x port-control 2/3 force-  
authorize
```

```
port 1/2 control was set to force-authorize
```

set port dot1x quiet-period

User level: supervisor

Use the `set port dot1x quiet-period` command to set the 802.1x quiet period per port.

The syntax for this command is:

```
set port dot1x quiet-period <module/port> <seconds>

  module/  Module and port number (or range of ports)
  port
  seconds  Number of seconds – 0 to 65535
```

Example:

```
P330-1(super)# set port dot1x quiet-period 4/2 300
```

set port dot1x re-authenticate

User level: supervisor

Use the `set port dot1x re-authenticate` command to set the port to re-authenticate.

The syntax for this command is:

```
set port dot1x re-authenticate <module/port>

  module/  Module and port number (or range of ports)
  port
```

Example:

```
P330-1(super)# set port dot1x re-authenticate 1/2
port 1/2 is not in authenticating process
```

set port dot1x re-authentication

User level: supervisor

Use the `set port dot1x re-authentication` command to set the re-authentication mode per port.

The syntax for this command is:

```
set port dot1x re-authentication <module/port> <mode>

  module/  Module and port number (or range of ports)
  port
  mode     enable | disable
```

Example:

```
P330-1(super)# set port dot1x re-authentication 1/2 enable  
port 1/2 re-authenticate was set to enable
```

set port dot1x re-authperiod

User level: supervisor

Use the `set port dot1x re-authperiod` command to set the the idle time between re-authentication attempts before the session is terminated.

The syntax for this command is:

```
set port dot1x re-authperiod <module/port> <seconds>
```

module/ Module and port number (or range of ports)

port

seconds Number of seconds – 0 to 65535

Example:

```
P330-1(super)# set port dot1x re-authperiod 1/2 400
```

set port dot1x server-timeout

User level: supervisor

Use the `set port dot1x server-timeout` command to set the time to wait for a reply from the Authentication Server before the session is terminated.

The syntax for this command is:

```
set port dot1x server-timeout <module/port> <seconds>
```

module/ Module and port number (or range of ports)

port

seconds Number of seconds – 0 to 65535

Example:

```
P330-1(super)# set port dot1x server timeout 1/2 400
```

set port dot1x supp-timeout

User level: supervisor

Use the `set port dot1x supp-timeout` command to set the time for the port to wait for a reply from the Authentication Server before the session is terminated.

The syntax for this command is:

```
set port dot1x supp-timeout <module/port> <seconds>
```

module/ Module and port number (or range of ports)

port

seconds Number of seconds – 0 to 65535

Example:

```
P330-1(super)# set port dot1x supp-timeout 1/2 400
```

set port dot1x tx-period

User level: supervisor

Use the `set port dot1x tx-period` command to set the time interval between attempts to access the Authenticated Station.

The syntax for this command is:

```
set port dot1x tx-period <module/port> <seconds>
```

module/ Module and port number (or range of ports)

port

seconds Number of seconds — 0-65535

Example:

```
P330-1(super)# set port dot1x quiet-period 1/2 5000
```

set port duplex

User level: privileged, supervisor.

Use the `set port duplex` command to configure the duplex type of an Ethernet or Fast Ethernet port or range of ports. You can configure Ethernet and Fast Ethernet interfaces to either full duplex or half duplex.

The duplex status of a port in auto-negotiation mode is determined by auto-negotiation. An error message is generated if you attempt to set the transmission type of auto negotiation Fast Ethernet ports to half- or full-duplex mode.

- ① P332G-ML and P332GT-ML ports and P334T-ML ports 51, 52 (Gigabit SFP ports) work in Full duplex mode only. An error message is generated if you attempt to change these ports to half-duplex.

The syntax for this command is:

```
set port duplex <module>/<port> {full|half}
```

module	Number of the switch in the stack. If you do not specify a number, the ports on all the switches are shown.
port	Number of the port on the module. If you do not specify a number, all the ports on the module are shown. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.
full	Set full-duplex transmission
half	Set half-duplex transmission

Example:

To set port 1 on module 4 to full duplex:

```
P330-N# set port duplex 4/1 full
```

```
Port 4/1 set to full-duplex.
```

set port edge admin state

User level: privileged, supervisor.

Use the `set port edge admin state` command to set the port as an RSTP edge-port or non-edge-port.

- ① You must manually configure uplink and backbone ports (including LAG logical ports) to be “non-edge” ports, using the CLI command `set port edge admin state`.

The syntax for this command is:

```
set port edge admin state <module/port> <admin state>
```

module/	Port identifier
port	

admin state The port's admin state can be set to either edge-port or non-edge-port.

Examples:

```
P330-N# set port edge admin state 1/1 edge-port  
port 1/1 edge admin state is set to edge-port
```

```
P330-N# set port edge admin state 1/1 non-edge-port  
port 1/1 edge admin state is set to non-edge-port
```

set port enable

User level: privileged, supervisor.

Use the `set port enable` command to enable a port or a range of ports.

The syntax for this command is:

```
set port enable [mod_num/port_num]
```

module Number of the switch.

port Number of the port on the switch.
You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example:

```
P330-N# set port enable 4/1  
Port 4/1 enabled.
```

set port flowcontrol

User level: privileged, supervisor.

Use the `set port flowcontrol` command to set the send/receive mode for flow-control frames (IEEE 802.3x or proprietary) for a full duplex port. Each direction (send or receive) can be configured separately.

The syntax for this command is:

```
set port flowcontrol {receive | send | all} <module/port> {off
```

```
| on | proprietary}
```

receive	Indicates whether the port can receive administrative status from a remote device. <i>Available only for Gigabit Ethernet modules with negotiation set to off.</i>
send	Indicate whether the local port can send administrative status to a remote device. <i>Available only for Gigabit Ethernet modules with negotiation set to off.</i>
all	Send and receive (symmetric flow control).
module	Number of the module.
port	Number of the port on the module.
off	Used with receive to turn off an attached device's ability to send flow-control packets to a local port. Used with send to turn off the local port's ability to send administrative status to a remote device.
on	Used with receive to require that a local port receive administrative status from a remote device. Used with send, the local port sends administrative status to a remote device.

Example:

```
P330-N# set port flowcontrol receive 5/1 on
```

```
Port 5/1 flow control receive administration status set to on
```

set port level

User level: privileged, supervisor.

Use the `set port level` command to set the priority level of a port or range of ports on the switching bus. Packets traveling through a port set at normal priority should be served only after packets traveling through a port set at high priority are served.

The syntax for this command is:

```
set port level <module>/<port> [value]
```

module	Number of the switch.
--------	-----------------------

port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.
value	Priority level (0-7)

Example:

```
P330-N# set port level 3/1 5
Port 3/1 level set to 5
```

set port mirror

User level: privileged, supervisor.

Use the `set port mirror` command to define a port mirroring pair in the stack.



Note: Ensure that the VLAN binding parameters are identical on the source and destination ports.

The syntax for this command is:

```
set port mirror source-port <module/port> mirror-port
<module/port> sampling <activate> direction <direction>
```

module	Number of the switch.
port	Number of the port on the switch.
activate	always - keyword to activate the port mirroring entry
direction	rx - keyword to copy only incoming traffic both - keyword to copy both incoming and outgoing traffic

Example:

```
P330-N# set port mirror source-port 3/9 mirror-port 4/10
sampling always direction both
Mirroring both Rx and Tx packets from port 3/9 to port 4/10
is enabled
```

set port name

User level: privileged, supervisor.

Use the `set port name` command to configure a name for a port. If you do not specify a name, the port name remains blank.

The syntax for this command is:

```
set port name <module>/<port> [<name>]
```

module	Number of the switch.
port	Number of the port on the switch.
name	Name (up to 16 characters)

Example:

```
P330-N# set port name 4/21 arthur

Port 4/21 name set.
```

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set port negotiation

User level: privileged, supervisor.

Use the `set port negotiation` command to enable or disable the link negotiation protocol on the specified port. This command is available on Fast Ethernet or Gigabit Ethernet ports.

When negotiation is enabled, the speed and duplex of the Fast Ethernet ports are determined by auto-negotiation.

If negotiation is disabled, the user can set the speed and duplex of the Fast Ethernet ports.

For Fiber Gigbit Ethernet ports it can determine the flow control (pause) mode only.

- ① Copper ports in the P332GT-ML can work at 1000Mbps (Full Duplex) only if autonegotiation is enabled on both cable ends and you are using a 4 pair (8 wires) Ethernet cable. If autonegotiation is disabled, these ports can only work at 100Mbps (Full Duplex), and autonegotiation should be disabled on both cable ends.

The syntax for this command is:

```
set port negotiation <module>/<port> {enable|disable}
```

module	Number of the switch. If you do not specify a number, the ports on all the switches are shown.
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.
enable	Enable port negotiation protocol
disable	Disable port negotiation protocol

Example:

To disable autonegotiation on port 1, module 4:

```
P330-N# set port negotiation 4/1 disable  
Link negotiation protocol disabled on port 4/1.
```

set port point-to-point admin status

User level: privileged, supervisor.

Use the `set port point-to-point admin status` command to set the port RSTP point-to-point admin status.

The syntax for this command is:

```
set port point-to-point admin status <module/port> <admin status>
```

module/ port	Port identifier
admin status	force-true - treat this port as if it is connected point-to-point force-false - treat this port as if it is connected to shared media auto - try to automatically detect the connection type of the port

Example:

```
P330-N# set port point-to-point admin status 1/1 force-true  
port 1/1 point to point admin status is set to force-true
```

set port powerline

User level: privileged, supervisor.

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `set port powerinline` command to enable or disable the load detection process and power delivery for the port.

The syntax for this command is:

```
set port powerinline <module_number/port_number> {[enable] |
disable}
```

`module_number` Number of the module hosting the port for which load detection is to be enabled/disabled.

`port_number` Number of the port for which load detection should be enabled/disabled.

`enable` - enables load detection process for port
`disable` - disables load detection process for port

Example:

```
P330-N# set port powerinline 3/1-3 enable
Load detection process on ports 3/1-3 is enabled
```

set port powerline priority

User level: privileged, supervisor.

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `set port power inline priority` command to configure the priority level of powering the port. Possible values are Critical, High, and Low. At power on all ports are set to Low Priority.

Within each group, the lowest port number has a highest priority, i.e. within the ports 1 to 8, port 1 has the highest priority although its priority is lower than port 9 which belongs to High priority group.

The syntax for this command is:

```
set port powerinline priority <module_number/port_number>
<priority>
```

`module_number` Number of the module hosting the port for which a powerline priority level is to be set.

`port_number` Number of the port for which a powerline priority level is to be set.

priority Critical, High, or Low

Example:

```
Router-N# set port powerinline priority 2/3 HighLoad  
Powering priority on port/s 2/3 was set to High
```

set port redundancy

User level: privileged, supervisor.

Use the `set port redundancy` command to globally enables or disable the port redundancy pairs you have defined. Using this command will not delete from NVRAM the existing redundancy entries.

The syntax for this command is:

```
set port redundancy {enable|disable}
```

Example:

```
P330-N# set port redundancy enable  
All redundancy schemes are now enabled
```

set port redundancy on/off

User level: privileged, supervisor.

Use the `set port redundancy` command to defines or remove redundancy pairs. A port redundancy member can be any port (including LAG logical port) that is not a member of a LAG or another redundancy scheme.

The syntax for this command is:

```
set port redundancy <module>/<prim_port>  
<module>/<second_port> {on/off} [<redundancy_name>]
```

prim_port	Primary port of the redundancy scheme
second_port	Secondary port of the redundancy scheme
redundancy_name (Optional)	Name for the redundancy scheme

Example:

```
P330-N# set port redundancy 1/7 2/12 on red1
uplink: Port 2/12 is redundant to port 1/7.

Port redundancy is active - entry is effective immediately
```

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set port redundancy-intervals

User level: privileged, supervisor.

Use the set port redundancy-intervals command to configure the two time constants that determine redundancy switchover parameters:

- “Min Time-between-switchovers” is the minimum interval between switchover of each pair.
- “Switchback-interval” is the period the primary port link has to be “up” before the system switches back.

If the switchback interval is zero, the system never switches back. If it is one, switchback occurs immediately after the primary port link returns.

The syntax for this command is:

```
set port redundancy-intervals <min-time-between-switchovers>
<switchback-interval> | none
```

min-time-between-switchovers	The minimum time between redundancy switchovers for each pair (in milliseconds).
switchback-interval	The period the primary port link has to be “up” before the system switches back (in milliseconds). <ul style="list-style-type: none"> • If switchback interval is zero, the switchback is immediate
none	The system switches back only if the secondary link fails.

Example:

```
P330-N# set port redundancy-intervals 100 20
```

set port security

User level: supervisor

Use the `set port security` command to enable MAC security on a port or a range of ports at the module level. The port security is activated only after you enable the security mode at the stack level using the `set security mode` command.

The syntax for this command is:

```
set port security { enable | disable } [<module>[/<port>]]
```

`enable | disable` Set the port security enable or disable

`module/port` The switch number/the port number

Example:

```
P330-1(super)# set port security enable 1/2  
Port 1/2 secured.
```

set port spantree cost

User level: privileged, supervisor.

Use the `set port spantree cost` command to set the cost of a port. This value defines which port will be allowed to forward traffic if two ports with different costs cause a loop.

The syntax for this command is:

```
set port spantree cost [module/port] [auto|value]
```

`module/port` Module number/port number.

`auto` Spantree cost is calculated according to the standard

`value` Number representing the cost. The cost level can be set from 1 to 65535 / 200000000 in STP / RSTP, respectively. A lower cost (lower value) specifies precedence of a port to forward traffic.

Example:

```
P330-N>set port spantree cost 4/2 4096  
port 4/2 spantree cost is 4096
```

set port spantree disable

User level: privileged, supervisor.

Use the `set port spantree disable` command to disable the spanning tree mode for specific switch ports.

The syntax for this command is:

```
set port spantree disable [module/port]
```

Module	Module number
--------	---------------

Port	Port number
------	-------------

Example:

```
P330-N# set port spantree disable 3/1
port 3/1 was disabled on spantree
```

set port spantree enable

User level: privileged, supervisor.

Use the `set port spantree enable` command to enable the spanning tree mode for specific switch ports.

The syntax for this command is:

```
set port spantree enable [module/port]
```

Module	Module number
--------	---------------

Port	Port number
------	-------------

Example:

```
P330-N# set port spantree enable 3/1
port 3/1 was enabled on spantree
```

set port spantree force-protocol-migration

User level: privileged, supervisor.

Use the `set port spantree force-protocol-migration` command to set the port as an RSTP port (and not as common STA port). It forces the port to send a rapid spanning tree BPDU.

The syntax for this command is:

```
set port spantree force-protocol-migration <module/port>  
  
  module/  Port identifier  
  port
```

Example:

```
P330-N>set port spantree force-protocol-migration 1/1  
port 1/1 is forced to send a Rapid spanning tree BPDU
```

set port spantree priority

User level: privileged, supervisor.

Use the `set port spantree` command to set the Spanning Tree priority level of a port. This value defines the priority of a port to be blocked in case two ports with the same costs cause a loop.

The syntax for this command is:

```
set port spantree priority [module/port] [value]
```

module/port	Module number/port number.
value	Number representing the priority of the bridge. The priority level is from 0 to 240, with 0 indicating high priority and 240 indicating low priority. Value should be in steps of 16; default value is 128.

Example:

```
P330-N# set port spantree priority 3/4 128  
port 3/4 spantree priority is 128
```

❶ Priority value 0 will set the port to Root port.

set port speed

User level: privileged, supervisor.

Use the `set port speed` command to configure the speed of a port or range of 10/100BASE-T ports.

In auto-negotiation mode, the port's speed is determined by auto negotiation. An error message is generated if you attempt to set the speed when auto negotiation is enabled

- ① This command is can not be executed for P332G-ML and P332GT-ML ports and P334T-ML ports 51, 52 (Gigabit SFP ports). An error message is generated if you attempt to perform the `set port speed` command for these ports that can only work at 1000Mbps speed.
- ① Copper ports in the P332GT-ML can work at 1000Mbps (Full Duplex) only if autonegotiation is enabled on both cable ends and you are using a 4 pair (8-wire) Ethernet cable. If autonegotiation is disabled, these ports can work only at 100 Mbps (Full Duplex), and autonegotiation must be disabled on both cable ends.

The syntax for this command is:

```
set port speed <mod_num>/<port_num> <10MB|100MB|1GB>
```

`mod_num` Number of the switch.

`port_num` Number of the port on the switch.
You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.

Example:

To configure port 1 on module 4 to 100 Mbps

```
P330-N# set port speed 4/1 100MB
```

```
Port 4/1 speed set to 100 Mbps.
```

set port static-vlan

User level: privileged, supervisor.

Use the `set port static-vlan` command to assign static VLANs to ports.

The syntax for this command is:

```
set port static-vlan [module/port range] [vlan num]
```

`module/port range` Port range

`vlan num` vlan to bind to port

Example:

```
P330-N# set port static-vlan 3/4-6 2
VLAN 2 is bound to port 3/4
VLAN 2 is bound to port 3/5
VLAN 2 is bound to port 3/6
```

set port trap

User level: privileged, supervisor.

Use the `set port trap` command to enable or disable generic SNMP uplink or downlink traps from a port.

The syntax for this command is:

```
set port trap <module>/<port> {enable|disable}
```

module	Number of the switch.
port	Number of the port on the switch. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.
enable	Enable uplink/downlink traps
disable	Disable uplink/downlink traps

Example:

```
P330-N# set port trap 3/2 enable
Port 3/2 up/down trap enabled.
```

set port vlan

User level: privileged, supervisor.

Use the `set port vlan` command to set the port VLAN ID (PVID). If adding a new VLAN, the VLAN number must be within the range 1 to 3071.

① You need to define a vlan before setting a port VLAN ID.

The syntax for this command is:

```
set port vlan <vlan_num> <module>/<port>
```

vlan_num	Number identifying the VLAN.
----------	------------------------------

module	The switch number
port	Number of the port on the switch. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.

Example:

To set VLAN 850 to include ports 4 through 7 on module 3.

```
P330-N# set port vlan 850 3/4-7

VLAN 850 modified.
VLAN  Mod/Ports
----  -
850   3/4-7
```

set port vlan-binding-mode

User level: privileged, supervisor.

Use the `set port vlan-binding-mode` command to define the binding method used by ports.

The syntax for this command is:

```
set port vlan-binding-mode [port_list] [value]
```

port list	Switches and ports to bundle (format: module/port)
value	<ul style="list-style-type: none"> static - the port supports only the VLAN as configured per port bind-to-configured - the port supports the VLANs configured on the device bind-to-all - the port support the whole range of VLANs on the device

Example:

```
P330-N# set port vlan-binding-mode 5/5-9 static
Set Port vlan binding method:5/5
Set Port vlan binding method:5/6
Set Port vlan binding method:5/7
Set Port vlan binding method:5/8
Set Port vlan binding method:5/9
```

set powerinline external power

User level: privileged, supervisor.

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `set powerinline external power` command to set the maximum power available from the external power supply to power DTEs.

The syntax for this command is:

```
set powerinline external power <module_number> <power>
```

<code>module_number</code>	Number of the module for which external power is to be allocated
<code>power</code>	Value of the maximum power allocated to powering DTEs in Watts.

Example:

```
P330-N# set powerinline external 2 200
external power set to 200Watts
```

set ppp authentication incoming

User level: privileged, supervisor.

Use the `set ppp authentication` command to define the authentication method used for a PPP server or client session.

The syntax for this command is:

```
set ppp authentication incoming {pap|chap|none}
```

<code>pap</code>	PAP authentication method
<code>chap</code>	CHAP authentication method
<code>none</code>	No authentication

Example:

```
P330-N# set ppp authentication incoming chap
PPP requires CHAP authentication for incoming sessions.
```


set ppp baud-rate

User level: privileged, supervisor.

Defines the baud rate used in PPP sessions.

① The peer baud rate must be set at the same value as the host.

The syntax for this command is:

```
set ppp baud-rate <9600|19200|38400>
```

Example:

```
P330-N# set ppp baud-rate 38400
ppp baud rate was set to 38400
```

set ppp chap-secret

User level: supervisor

Use the `set ppp chap-secret` command to configure the “shared secret” used in PPP sessions with CHAP authentication. The chap-secret is not transferable via the configuration upload/download mechanism.

The syntax for this command is:

```
set ppp chap-secret <chap-secret>
```

chap-secret The shared secret, 4 to 32 characters.

Example:

```
P330-1(super)# set ppp chap secret hush
PPP shared secret for CHAP authentication is set
```

set ppp incoming timeout

User level: privileged, supervisor.

Use the `set ppp incoming timeout` command to set the number of minutes until the system automatically disconnects an idle PPP incoming session.

The syntax for this command is:

```
set ppp incoming timeout <time>
```

time The timeout in minutes

Example:

```
P330-N# set ppp incoming timeout 15  
PPP incoming session will automatically disconnect after 15  
minutes of idle time
```

set psu type

User level: privileged, supervisor.

Use the `set psu type` command to set the main power supply type (AC/DC) of the module.

- ❶ This command is not applicable to P330-ML-ML switches, which determine the PSU type automatically. This command is used to set the power supply types for other P330-ML switches in the stack.

The syntax for this command is:

```
set psu type [AC|DC] [module number]
```

Example:

```
P330-N# set psu type DC 3  
Power supply type was changed to DC on module 3
```

set qos policy-source

User level: supervisor

- ❶ This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `set qos policy-source` command to set the policy source (local or policy server).

The syntax for this command is:

```
set policy source <source>
```

source local or policy server

- The default policy source for the P334T-ML switch is *local*

Example:

```
P330-N# set qos policy-source local  
Done!
```

set queuing scheme

User level: privileged, supervisor.

① This command is applicable to P330-ML-ML switches only.

Use the `set queuing scheme` command to set the queuing scheme to either strict or weighted round robin and to set the weights.

The syntax for this command is:

```
set queuing scheme {wrr {H} | strict | default} [module]
```

`wrr/strict /default` Sets queuing scheme to weighted round robin, strict, or the default.

`H` Ratio between high and low priority queues. This parameter is only used when the queuing scheme is weighted round robin.

`module` The module number to which the queuing scheme applies. If no module is specified, the command affects all P330-ML-ML modules in the stack.

Examples:

```
P330-N# set queuing scheme wrr 10 2
Module Queuing Scheme
-----
      2  Wrr 10:1

P330-N# set queuing scheme default
Module Queuing Scheme
-----
      1  Default
      2  Default
```

set radius authentication enable/disable

User level: privileged, supervisor.

Enables or disables RADIUS authentication for the P330-ML switch.

The syntax for this command is:

```
set radius authentication {enable|disable}
```

enable Enable RADIUS authentication

disable Disable RADIUS authentication (default)

Example:

```
P330-1 (super) # set radius authentication enable
```

set radius authentication retry-number

User level: privileged, supervisor.

Sets the number of times an access request is sent when there is no response.

The syntax for this command is:

```
set radius authentication retry-number <number>
```

number Number of retries

Example:

```
P330-1 (super) # set radius authentication retry-number 3
```

set radius authentication retry-time

User level: privileged, supervisor.

Sets the time to wait before re-sending an access request.

The syntax for this command is:

```
set radius authentication retry-time <time>
```

time Retry time in seconds

Example:

```
P330-1 (super) # set radius authentication retry-time 5
```

set radius authentication secret*User level: supervisor*

Use the `set radius authentication secret` command to enable secret authentication for the P330-ML unit.

The syntax for this command is:

```
set radius authentication secret <string>
string text password
```

Example:

```
P330-1(super)# set radius authentication secret hush
```

set radius authentication server*User level: privileged, supervisor.*

Sets the IP address (and shared secret) of the primary or secondary RADIUS Authentication server.

The syntax for this command is:

```
set radius authentication server <ip-addr> {primary |
secondary}
```

ip-addr	IP address of the RADIUS authentication server
primary	default - Primary authentication server
secondary	Secondary authentication server

Example:

```
P330-1(super)# set radius authentication server
192.40.12.36 primary
```

set radius authentication udp-port*User level: privileged, supervisor.*

Use the `set radius authentication udp-port` command to set the RFC 2138 approved UDP port number.

Normally, the UDP port number should be set to its default value of 1812. Some early implementations of the RADIUS server used port number 1645.

The syntax for this command is:

```
set radius authentication udp-port <number>
```

Example:

```
P330-1(super)# set radius authentication udp-port 300
```

set secure mac

User level: privileged, supervisor.

Use the `set secure mac` command to add a unicast MAC address into the CAM table of a secured port.

The syntax for this command is:

```
set secure mac <mac-address> port <mod-num>/<port-num>
```

Example:

```
P330-1(super)# set secure mac 00-02-03-04-04-05 port 1/1  
Port 1/1 port security enabled with 00-02-03-04-04-05 as  
the secure mac address
```

set security mode

User level: privileged, supervisor.

Use the `set security mode` command to enable or disable MAC security at the stack level. When enabled, the ports are secured based on their individual configuration. When disabled, all the ports in a stack are non-secured.

The syntax for this command is:

```
set security mode {enable|disable}
```

Example:

```
P330-1(super)# set security mode enable  
Security mode enabled.
```

set security violation

User level: user, privileged, supervisor

Use the `set security violation` command to specify the security violation action to be taken.

① This command is only available on P330-ML-ML switches.

The syntax for this command is:

```
set security violaton action {restrict|restrict-and-notify}
```

restrict	Keyword specifying that the port drops all packets from insecure hosts but remains enabled.
restrict-and-notify	Keyword specifying that the port drops all packets and sends an SNMP trap.

Example:

```
P330-1(super)# set security violation action restrict  
Switch security violation action restrict
```

set snmp community

User level: privileged, supervisor.

Use the `set snmp community` command to set or modify the switch's SNMP community strings.

The syntax for this command is:

```
set snmp community <read-only | read-write | trap> [community string]
```

Example:

```
P330-N# set snmp community read-only read  
SNMP read-only community string set
```

set snmp retries

User level: privileged, supervisor.

Use the `set snmp retries` command to set the number of retries initiated by the P330-ML Manager when it tries to send SNMP messages to the switch.

The syntax for this command is:

```
set snmp retries <number>
```

number	Number of retries
--------	-------------------

Example:

```
P330-N# set snmp retries 10
SNMP retries is set to 10
```

set snmp timeout

User level: privileged, supervisor.

Use the `set snmp timeout` command to set the SNMP timeout in seconds. This command is only used for access using the P330-ML Embedded Web Manager.

The syntax for this command is:

```
set snmp timeout <number>
```

number	Timeout in seconds
--------	--------------------

Example:

```
P330-N# set snmp timeout 2000
the SNMP Timeout is set to 2000
```

set snmp trap

User level: privileged, supervisor.

Use the `set snmp trap` command to add an entry into the SNMP trap receiver table and to enable or disable the different SNMP traps for a specific receiver.

First add the `rcvr_addr` and then enable/disable the different traps for it.

The syntax for this command is:

```
set snmp trap <rcvr_addr>
set snmp trap <rcvr_addr> {enable|disable}
{all|config|fault|...}
```

enable	Activate SNMP traps
disable	Deactivate SNMP traps
all	(Optional) Specify all trap types
config	(Optional) Specify the ConfigChange trap from the TRAP-MIB.
fault	(Optional) Specify the Fault trap from the TRAP-MIB.
rcvr_addr	IP address or IP alias of the system to receive SNMP traps

Example:

To enable SNMP ConfigChange traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 enable config  
SNMP config change traps enabled.
```

Example:

To enable all traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 enable all  
SNMP all traps enabled.
```

Example:

To disable SNMP config traps to a specific manager:

```
P330-N# set snmp trap 192.168.173.42 disable config  
SNMP config traps disabled.
```

Example:

To add an entry in the SNMP trap receiver table with default:

```
P330-N# set snmp trap 192.168.173.42  
SNMP trap receiver added.
```

set snmp trap auth

User level: privileged, supervisor.

Use the `set snmp trap auth` command to enable or disable the sending of SNMP traps upon SNMP authentication failure.

The syntax for this command is:

```
set snmp trap {enable|disable} auth
```

Example:

```
P330-N# set snmp trap enable auth  
Authentication trap enabled
```

set spantree default-path-cost

User level: privileged, supervisor.

Use the `set spantree default-path-cost` command to set the version of the spanning tree default path costs that are to be used by this bridge.

The syntax for this command is:

```
set spantree default-path-cost <path-cost>
```

path-cost	common-spanning-tree - compatible with ieee802.1D standard rapid-spanning-tree - compatible with ieee802.1W standard
-----------	---

Example:

```
P330-N# set spantree default-path-cost rapid-spanning-tree
Spanning tree default path costs is set to rapid spanning
tree.
```

set spantree disable

User level: privileged, supervisor.

Use the `set spantree disable` command to disable the spanning-tree algorithm for the switch.

- ① When you disable STP, blocking ports are disabled in order to prevent loops in the network. As a result, you need to wait 30 seconds before disabling STP if you reset the switch, enable STP, or insert a new station.

The syntax for this command is:

```
set spantree disable
```

Example:

```
P330-N# set spantree disable
bridge spanning tree disabled.
```

set spantree enable

User level: privileged, supervisor.

Use the `set spantree enable` command to enable the spanning-tree algorithm for the switch.

- ① When you disable STP, blocking ports are disabled in order to prevent loops in the network. As a result, you need to wait 30 seconds before disabling STP if you reset the switch, enable STP, or insert a new station.

The syntax for this command is:

```
set spantree enable
```

Example:

```
P330-N# set spantree enable  
bridge spanning tree enabled.
```

set spantree forward-delay

User level: privileged, supervisor.

Use the `set spantree forward-delay` command to set the bridge forward delay time parameter.

The syntax for this command is:

```
set spantree forward-delay <time>
```

`forward -` The time that is used when transferring the port to forwarding state.
`delay` Value range is 4-30 and must exceed (Bridge Max Age/2).
Recommended value is 15 seconds.

Example:

```
P330-N# set spantree forward-delay 15  
bridge forward delay set to 15.
```

set spantree hello-time

User level: privileged, supervisor.

Use the `set spantree hello-time` command to set the bridge hello time parameter.

The syntax for this command is:

```
set spantree hello-time <time>
```

`hello-time` The time interval (in seconds) between the generation of configuration BPDUs by the Root. Value ranges between 1 to 10 and must not exceed (Bridge-Max-Age/2) - 1.
The recommended value is 2 sec.

Example:

```
P330-N# set spantree hello-time 2  
bridge hello time set to 2.
```

set spantree max-age

User level: privileged, supervisor.

Use the `set spantree max-age` command to set the bridge spanning tree max age parameter.

The syntax for this command is:

```
set spantree max-age <seconds>
```

max-age The max age time in seconds to keep message information before it is discarded. Value ranges between 6 to 40; value must be between 2 X (Bridge-Hello-Time + 1) and 2 X (Bridge-Forward-Delay - 1). Recommended value is 20 sec.

Example:

```
P330-N# set spantree max-age 20  
bridge max age is set to 20.
```

set spantree priority

User level: privileged, supervisor.

The syntax for this command is:

```
set spantree priority <number>
```

number The priority level is from 0 to 61440, with 0 indicating high priority and 61440 indicating low priority; value should be in steps of 4096. Default value is 32768.

Example:

```
P330-N# set spantree priority 4096  
Bridge priority set to 4096.
```

set spantree tx-hold-count

User level: privileged, supervisor.

Use the `set spantree tx-hold-count` command to limit the maximum number of BPDUs transmitted during a hello-time period.

The syntax for this command is:

```
set spantree tx-hold-count <rate>
```

rate Value between 1 to 10; recommended value is 3

Example:

```
P330-N# set spantree tx-hold-count 3  
tx hold count is set to 3.
```

set spantree version

User level: privileged, supervisor.

Use the `set spantree version` command to set the rapid spanning tree state machine to work as "STP compatible".

The syntax for this command is:

```
set spantree version <version>
```

version common-spanning-tree — compatible with ieee802.1D standard.
 rapid-spanning-tree — compatible with ieee802.1W standard

Example:

```
P330-N# set spantree version rapid-spanning-tree  
Spanning tree version is set to rapid spanning tree.
```

set system contact

User level: privileged, supervisor.

Use the `set system contact` command to set the mib2 system contact MIB variable.

The syntax for this command is:

```
set system contact [string]
```

- | | |
|--------|---|
| string | <ul style="list-style-type: none"> • The contact name string should be typed inside inverted commas. • The name is cleared if you leave this field blank. |
|--------|---|

Example:

```
P330-1(super)# set system contact "gregory kohll"
*** Set system contact ***

system contact set
```

set system location

User level: privileged, supervisor.

Use the `set system location` command to set the mib2 system location MIB variable

The syntax for this command is:

```
set system location [string]
```

- | | |
|--------|--|
| string | <ul style="list-style-type: none"> • The location name string should be typed inside inverted commas. • The location is cleared if you leave this field blank. |
|--------|--|

Example:

```
P330-N# set system location "tech-support"
*** Set system location ***

system location set
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

set system name

User level: privileged, supervisor.

Use the `set system name` command to set the mib2 system name MIB variable.

The syntax for this command is:

```
set system name [string]
```

- | | |
|--------|---|
| string | <ul style="list-style-type: none">• The system name string should be typed inside inverted commas.• The name is cleared if you leave this field blank. |
|--------|---|

Example:

```
P330-N# set system name "P330-ML-1"  
*** Set system name ***  
  
system name set
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

set terminal recovery password disable

User level: supervisor

Use the `set terminal recovery password disable` command to disable the recovery password feature.

- ① This command can only be run from the console port on the device.
- ① If the recovery password feature is disabled and you forget your login and password, you will not be able to access the device.

The syntax for this command is:

```
set terminal recovery password disable
```

Example:

```
P330-N# set terminal recovery password disable  
Done!
```

set terminal recovery password

User level: supervisor

Use the `set terminal recovery password enable` command to enable the recovery password feature.

① This command can only be run from the console port on the device.

The syntax for this command is:

set terminal recovery password enable

Example:

```
P330-N# set terminal recovery password enable
Done!
```

set time client

User level: privileged, supervisor.

Use the `set time client` command to enable or disable the periodic network time acquisition by the switch from the network time server (SNTP or TIME protocol).

The syntax for this command is:

```
set time client {enable|disable}
```

enable Enable periodic network time acquisition

disable Disable periodic network time acquisition

Example:

```
P330-N# set time client enable
Time client mode enabled
```

set time protocol

User level: privileged, supervisor.

Use the `set time protocol` command to set the protocol for use in the system as either SNTP protocol or TIME protocol.

The syntax for this command is:

```
set time protocol [sntp-protocol|time-protocol]
```

sntp-protocol Use the SNTP protocol

time-protocol Use the TIME protocol

Example:

```
P330-N>set time protocol sntp-protocol
The protocol has been set to SNTP protocol

P330-N> set time protocol time-protocol
The protocol has been set to TIME protocol
```

set time server

User level: privileged, supervisor.

Use the `set time server` command to set the TIME server address.

The syntax for this command is:

```
set time server <ip address>
```

`ip address` IP address of the TIME server.

Example:

```
P330-N# set time server 192.49.53.68
The Server Ip has been set to 192.49.53.68
```

set timezone

User level: privileged, supervisor.

Use the `set timezone` command to assign a timezone name and sets the time difference of the device relative to the Coordinated Universal Time (UTC / GMT).

The `minutes` parameter can only be set to 30.

The syntax for this command is:

```
set timezone <zone-name> [-]<hours>[:30]
```

`zone-name` Three-character name of time zone, for example, EST, GMT

`hours` The difference between the time zone and GMT

Example:

```
P330-N# set timezone EST -5
Timezone set to "EST", offset from UTC is -5 hours.
```

set trunk

User level: privileged, supervisor.

Use the `set trunk` command to configure the VLAN tagging mode of a port.

```
set trunk <module/port> {off|dot1q}
```

module	Number of the switch.
port	Number of the port on the switch. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.
off	Forces the port to become a non-tagging port.
dot1q	Specifies an IEEE 802.1Q tagging on a Fast Ethernet or Gigabit Ethernet port.

Example:

```
P330-ML-1# set trunk 3/3 dot1q
Dot1Q VLAN tagging set on port 3/3.
```

set utilization cpu

User level: privileged, supervisor.

Use the `set utilization cpu` command to enable CPU utilization monitoring on the specified module.

The syntax for this command is:

```
set utilization cpu <module-number>
```

module-number	The module number for which CPU utilization monitoring is enabled.
---------------	--

Example:

```
P330-N# set utilization cpu 1
CPU utilization is set on module 1
Done!
```

set vlan

User level: privileged, supervisor.

Use the `set vlan` command to configure VLANs.

The syntax for this command is:

```
set vlan <vlan-id> [name <vlan-name>]
```

vlan-id vlan number

vlan-name vlan name

Example:

```
P330-N# set vlan 3 name gregory  
  
VLAN id 3, vlan-name gregory created.
```

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set web aux-files-url

User level: privileged, supervisor.

Use the `set web aux-files-url` command to allow the Device Manager to automatically locate the URL of the Web server containing the Device Manager help files and Java plug-in.

Tip: Ensure that the Web server is always accessible to prevent potential delays to Web access to the device.

The syntax for this command is:

```
set web aux-files-url <//IP address/directory name>
```

Example:

```
P330-N# set web aux-files-url //192.168.47.25/emweb-aux-  
files
```

- ① If you wish to define a directory name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set welcome message

User level: privileged, supervisor.

Use the `set welcome message` command to set a welcome message to appear after a reboot or after opening a new session (see `session` command) in the stack.

The syntax for this command is:

```
set welcome message [string]
```

`string` `string` - The string to be used as the welcome message.
 `blank` - Restores the default string.

Example:

```
P330-N# set welcome message avaya  
The new welcome string is "avaya"
```

- ① If you wish to define a string which includes spaces, you must enclose the entire string in quotation marks, e.g. "new york".

show allowed managers status

User level: user, privileged, supervisor

Use the `show allowed managers status` command to display the activation status of the Allowed Managers feature.

The syntax for this command is:

```
show allowed managers status
```

Example:

```
P330-1(super)# show allowed managers status  
  
Managers are disabled.
```

show allowed managers table

User level: user, privileged, supervisor

Use the `show allowed managers table` to display the list of the twenty possible allowed managers IP addresses.

The syntax for this command is:

```
show allowed managers table
```

Example:

```
P330-1(super)# show allowed managers table
1 ) 149.49.32.134
2 ) Not Used
3 ) Not Used
4 ) Not Used
5 ) Not Used
6 ) Not Used
7 ) Not Used
8 ) Not Used
9 ) Not Used
10) Not Used
11) Not Used
12) Not Used
13) Not Used
14) Not Used
15) Not Used
16) Not Used
17) Not Used
18) Not Used
19) Not Used
20) Not Used
```

show arp-aging-interval

User level: privileged, supervisor.

Use the `show arp-aging-interval` command to display the ARP table aging interval for table entries.

The syntax for this command is:

```
show arp-aging-interval
```

Example:

```
P330-N>show arp-aging-interval
ARP table aging interval was set to 10 minutes.
```

show arp-tx-interval

User level: privileged, supervisor.

Use the `show arp-tx-interval` command to display the keep-alive frames transmission interval.

The syntax for this command is:

```
show arp-tx-interval
```

Example:

```
P330-N>show arp-tx-interval  
  
ARP tx interval is set to 5 seconds.
```

show autopartition

User level: privileged, supervisor.

Use the `show autopartition` command to display the automatic partition.

- ① Autopartition for the P330-ML-ML switches will always have the value disabled. This command is used to display the autopartition status for the other P330-ML switches in the stack.

The syntax for this command is:

```
show autopartition [module]
```

Example:

```
P330-N>show autopartition 1  
  
Mod      Mode  
-----  
1        Enable
```


show boot bank

User level: privileged, supervisor.

① This command is not supported by the P333R and P333R-LB switches.

Use the `show boot bank` command to display the software bank from which the switch will boot at the next boot process.

You must issue this command separately for each switch in the stack using the `session` command.

① If you wish to run this command on a switch other than the stack master, you need to open a session to the relevant switch.

The syntax for this command is:

show boot bank

Example:

```
P330-N>show boot bank
Boot bank set to bank-a
```

show cam

User level: user, privileged, supervisor

Use the `show cam` command to either display the module and port number where a specific MAC address was learned, or the MAC addresses learned on a specific module and port.

① MACs associated with LAGs appear under the LAG ID, not under the LAG port.

The syntax for this command is:

```
show cam [module[/port]]
```

module (Optional)	Number of the switch. If you do not specify a number, all switches in the stack are shown.
----------------------	--

port (Optional)	Number of the port on the module. If you do not specify a number, all ports on the specified switch are shown.
--------------------	--

Example: (by Module/Port)

```

P330-N>show cam 1/1
show cam 1/1
Dest MAC/Route Dest Destination Ports
-----
00-40-0d-59-03-78 1/1
00-d0-79-0a-0a-da 1/1
00-40-0d-43-1e-e9 1/1
...
00-40-0d-c6-24-01 1/1
Total Matching CAM Entries Displayed = 178

```

show cam mac

User level: user, privileged, supervisor

Use the `show cam mac` command to display the module and port number where a specific MAC address was learned.

- ① MACs associated with LAGs appear under the LAG ID, not under the LAG port.

The syntax for this command is:

show cam mac <mac-addr>

mac-addr MAC address to search for.

Example:

```

P330-N# show cam mac 00-00-81-01-23-45
Dest MAC/Route Dest Destination Ports VLAN
-----
00-a0-cc-66-4e-52 1/8 1
Total Matching CAM Entries Displayed = 1

```

show cam vlan

User level: user, privileged, supervisor

Use the `show cam vlan` command to display the MAC addresses learned on a specific VLAN. The MAC addresses are displayed with their destination module and port number.

- ① MACs associated with LAGs appear under the LAG ID, not under the LAG port.

The syntax for this command is:

```
show cam vlan <vlan-number>
```

vlan-number The VLAN on which the MAC addresses were learned.

Example:

```
P330-N# show cam vlan 1
Please be patient.
Gathering and displaying the information might take a
while.
Dest MAC/Route Dest Destination Ports VLAN
-----
08-00-20-c4-c8-51 1/8 1
08-00-20-c6-98-5f 1/8 1
00-01-02-9b-ee-ae 1/8 1
00-01-02-dd-2f-9f 1/8 1
00-02-2d-47-00-6f 1/8 1
...
...
...
00-50-da-74-71-93 1/8 1
00-50-da-de-75-ca 1/8 1
00-60-08-96-25-20 1/8 1
Total Matching CAM Entries Displayed = 138
```

show cascading fault-monitoring

User level: user, privileged, supervisor

Use the `show cascading fault-monitoring` command to display the status of the fault trap sending mode for cascading links.

The syntax for this command is:

```
show cascading fault-monitoring [<mod_num>]
```

Example:

```
P330-N>show cascading fault-monitoring 1
Module 1 cascading-down fault monitoring enabled.
Module 1 cascading-up fault monitoring enabled.
```

show copy status

User level: user, privileged, supervisor

Use the `show copy status` command to show the status of the local configuration copy operation.

The syntax for this command is:

```
show copy status
```

Example:

```
Router-N> show copy status
Module #1
=====
Module           : 1
Source file      : .router-startup
Destination file : .router-running
Host            : -
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

show dev log file

User level: privileged, supervisor.

❶ This command applies the P330-ML-ML switches only.

Use the `show dev log file` command to display the encrypted device's log file.

The syntax for this command is:

```
show dev log file
```

Example:

```
P330-N>show dev log file

iW}ZH~YL{ }Z (^E^M)=}EsZ^E}Z
ZH~YL{ }Zj^M}ZZZZZZDZ (" "0Ji HA
Zl {~=ZNLMR}EZZZZZZDZw
Zl~' =; ^E}ZK}Esz~NZDZ@:3 :<w
Z!lZjLMR}EZZZZZZZZDZw:3
ZiW}Zl^>}YZn^=^ZzsDZ
ZZZZZZZZZZZZZZ
```

show device-mode

User level: user, privileged, supervisor

Use the `show device-mode` command to show the current P330-ML-ML or P333R operating mode. Possible modes are Router, or Layer 2.

- ① This command is not available to the P333T, P334T, P332MF and P333T-PWR switches which do not have Router and to P333R-LB which is always in Load-Balancing mode.

The syntax for this command is:

```
show device-mode
```

Example:

```
P330-N>show device mode
Device mode is router
```

show dot1x

User level: user, privileged, supervisor

Use the `show dot1x` command to display the system dot1x capabilities, protocol version, and timer values.

The syntax for this command is:

```
show dot1x
```

Example:

```
P330-N>show dot1x mode
PAE Capabilities           Authenticator Only
Protocol Version           1
system-auth-control        disabled
*** Warning : Authentication server ( RADIUS ) is
disabled/not-exist and so,
*** no authentication can be made
```

show download status

User level: user, privileged, supervisor

- ① This command applies to the P330-ML-ML switches only.

Use the `show download status` command to display a summary of the last software download operation.

The syntax for this command is:

```
show download status [slot]
```

Example:

```
P330-N>show download status 1
Module #1
=====
Module           : 1
Source file      : c:\session4.txt
Destination file : module-config
Host             : 149.49.75.100
Running state    : Idle
Failure display  : SCP - Server refused
Last warning     : No-warning
Bytes Downloaded : 0
```

show erase status

User level: user, privileged, supervisor

Use the `show erase status` command to view the status of the erase configuration operation.

The syntax for this command is:

```
show erase status
```

show image version

User level: user, privileged, supervisor

Use the `show image version` command to display the software version of the image on both memory banks of a specified switch.

The syntax for this command is:

```
show image version [<mod_num>]
```

If no switch number is specified, the image version of the all switches will be displayed.

Example:

```
P330-N>show image version 1
Mod      Module-Type                               Bank  Version
-----  -
1        24x10/100Base-T with optional expansion slot   A     4.0.3
1        24x10/100Base-T with optional expansion slot   B     4.0.3
```

show intelligent-multicast

User level: user, privileged, supervisor

Use the `show intelligent-multicast` command to display the intelligent multicast configuration.

The syntax for this command is:

```
show intelligent-multicast
```

Example:

```
P330-N>show intelligent-multicast
Intelligent-multicast configuration:
-----
intelligent-multicast state ----- Disabled
Intelligent-multicast client-port-pruning time ---      600[Sec]
Intelligent-multicast router-port-pruning time ---     1800[Sec]
intelligent-multicast group-filtering-delay time -       10[Sec]
```

show intelligent-multicast hardware-support

User level: user, privileged, supervisor

Use the `show intelligent-multicast hardware-support` command to display the intelligent multicast hardware support configuration.

The syntax for this command is:

```
show intelligent-multicast hardware-support
```

Example:

```
P330-N>show intelligent-multicast hardware support
Intelligent-multicast HW configuration:
#  Module           Sub-Module           Cascade
-----
1  Support IPMc     Not Installed        Support IPMc
```

show interface

User level: user, privileged, supervisor

Use the `show interface` command to display information on network interfaces.

The syntax for this command is:

```
show interface
```

Example:

P330-N> show interface				
Interface Name	Status	VLAN	IP address	Netmask
-----	-----	----	-----	-----
inband	disabled	1	135.64.200.105	255.255.255.0
ppp	disabled	N/A	0.0.0.0	0.0.0.0

show intermodule port redundancy

User level: user, privileged, supervisor

Use the `show intermodule redundancy` command to display the intermodule port redundancy entry defined for the stack.

The syntax for this command is:

```
show intermodule port redundancy
```

Example:

P330-N> show intermodule port redundancy	
Primary-Port	: 1/1
Primary-Port status	: Disable
Secondary-Port	: 1/2
Secondary-Port status	: Disable

show internal buffering

User level: user, privileged, supervisor

Use the `show internal buffering` command to display the size options (Maximum, Minimum, or Medium) of the Receive (Rx) buffer allocated to each port of the specified switch.

- ① Internal buffering for the P330-ML-ML switches will always have the value `Not supported`. This command is used to display the internal buffering status for the other P330-ML switches in the stack

The syntax for this command is:

show internal buffering [<mod_num>]

mod_num Switch number. If you do not specify a number then the internal buffering for all switches in the stack will be displayed.

Example:

```
P330-N>show internal buffering 1
Module  Internal Buffer
-----  -
      1           med
```

show ip access-group

User level: privileged, supervisor.

Use the `show ip access-group` command to display the active policy-list number.

① This command applies to the P334T-ML only when it is in device mode "Layer2".

The syntax for this command is:

`show ip access-group <policy-list-number>`

policy-list-number A valid id number for a policy list currently defined for the module.

Example:

```
P330-1 (super) # show ip access group 1011
access-group 101
```

show ip access-list details

User level: user, privileged, supervisor

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `show ip access-lists details` command to view complete data of a policy list (including DSCP and composite operation tables).

The syntax for this command is:

```
show ip access-list-details <policy-list-number>
```

policy-
list-
number A valid id number for a policy list currently defined for the module
(100 to 199, 0 is the default list)

Example:

```
P330-N>show ip access-list-details 101
Trust configuration is trust-cos
DSCP      Action          Precedence      Name
-----
0         fwd0              mandatory      DSCP#0
1         fwd0              mandatory      DSCP#1
2         fwd0              mandatory      DSCP#2
3         fwd0              mandatory      DSCP#3
4         fwd0              mandatory      DSCP#4
5         fwd0              mandatory      DSCP#5
6         fwd0              mandatory      DSCP#6
7         fwd0              mandatory      DSCP#7
8         fwd1              mandatory      DSCP#8
9         fwd1              mandatory      DSCP#9
10        fwd1              mandatory      DSCP#10
11        fwd1              mandatory      DSCP#11
```

show ip access-list-dscp

User level: user, privileged, supervisor

① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `show ip access-list-dscp` command to display the DSCP to CoS map of a policy-list.

The syntax for this command is:

```
show ip access-list-dscp <policy-list-number>
```

policy-
list-
number A valid id number for a policy list currently defined for the module
(100..199, 0 - default list)

dscp dscp entry (0 - 63)

Example:

```
P330-N>show ip access-list-dscp 101
Trust configuration is trust-cos
DSCP      Action                Precedence      Name
-----  -
0         fwd0                    mandatory      DSCP#0
1         fwd0                    mandatory      DSCP#1
2         fwd0                    mandatory      DSCP#2
3         fwd0                    mandatory      DSCP#3
4         fwd0                    mandatory      DSCP#4
5         fwd0                    mandatory      DSCP#5
6         fwd0                    mandatory      DSCP#6
7         fwd0                    mandatory      DSCP#7
8         fwd1                    mandatory      DSCP#8
9         fwd1                    mandatory      DSCP#9
10        fwd1                    mandatory      DSCP#10
11        fwd1                    mandatory      DSCP#11
```

show ip access lists

User level: user, privileged, supervisor

Use the `show ip access lists` command to display all the current policy lists.

① This command applies to the P334T-ML only, when it is in device mode "Layer2".

The syntax for this command is:

```
show ip access-lists[<policy-list-number>]
```

`policy-list-number` The policy list number (integer from 100 to 199; 0 is the default list).

Example:

```
Router-N> show ip access-lists
The current policy source is local
default List (0) parameters
List Owner : other
List 0 is valid
default action for list 0 is permit
```

show ip access-list-summary

User level: user, privileged, supervisor

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `show ip access-list-summary` command to display a summary of policy lists.

The syntax for this command is:

```
show ip access-list-summary
```

Example:

```
P330-N>show ip access-list-summary
The policy lists summary:
default List (0)
```

show ip route

User level: user, privileged, supervisor

Use the `show ip route` command to display IP routing table entries.

The syntax for this command is:

```
show ip route
```

Example:

```
P330-N>show ip route
Destination          Gateway
-----
0.0.0.0              149.49.54.1
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
0.0.0.0              0.0.0.0
```

show ip ssh

User level: supervisor

Use the `show ip ssh` command to display active SSH connections.

The syntax for this command is:

show ip ssh

Example:

```
P330-N>show ip ssh

Ssh Engine: Enable
Max Sessions: 2
Key Type: DSA , 768 bit
Listen Port: 22
Ciphers List: 3des-cbc
Session-Id  Version  Encryption  User      IP:Port
0x508622f0    2      3des-cbc   root     135.64.100.73:4201
```

show l2-module-config

User level: privileged, supervisor.

Use the `show l2-module-config` command to display Layer 2 module configuration.

- ① If this command is to be implemented on a switch other than the stack master, a session should be opened to the relevant switch.

The syntax for this command is:

`show l2-module-config`

Example:

```
P330-N>show 12-module-config

Please be patient.
Gathering and displaying the information might take a
while.

P330-ML-N(super)# !#
!# Upload time:                Unavailable Unavailable
!# System description:        Avaya Inc. - P330-ML
!# Master position:           2
!#
!# Module #:                   2
!# Module type, expansion type: P334T-ML-AC
!# Module-CS, expansion-CS:    1.0
!# MAC address:               00-40-0d-e5-e0-00
!# Serial #:                   4531636
!# SW versions - bank A, B, Boot: 4.0.15 4.2.5 3.11.0
!# Number of ports:           50
!#
!#
set port channel 2/30 on "qq"
!#
!#
!# Set queuing scheme parameters.

!#

set queuing scheme wrr 10 2

set cascading up fault-monitoring disable 2

set port spantree disable 2/5

set port edge admin state 2/52 non-edge-port

set port trap 2/1 disable

set port disable 2/1

set port classification 2/2 valuable
```

```
....  
....  
set port negotiation 2/11 disable  
set port duplex 2/11 half  
set port disable 2/15  
set port negotiation 2/31 disable  
set trunk 2/40 dot1q  
set trunk 2/44 dot1q  
set port vlan 500 2/44  
set trunk 2/51 dot1q  
set port dot1x port-control 2/2 force-authorize  
set port dot1x port-control 2/18 force-authorize  
set secure mac 00-00-01-02-02-02 port 2/5  
set secure mac 00-10-5a-0f-5e-1c port 2/11  
set port security enable 2/2  
set port security enable 2/10  
set port vlan-binding-mode 2/42 bind-to-configured  
set port vlan-binding-mode 2/44 bind-to-all
```

show l2-stack-config

User level: privileged, supervisor.

Use the `show l2-stack-config` command to display Layer 2 stack configuration.

- ① If this command is to be implemented on a switch other than the stack master, a session should be opened to the relevant switch.

The syntax for this command is:

```
show l2-stack-config
```


Example:

```
P330-N>show 12-stack-config

P330-ML-N(super)# !#

!# Upload time:                Unavailable Unavailable
!# System description:         Avaya Inc. - P330-ML
!# IP address, netmask:        149.49.138.157 255.255.255.0
!# Master position:            2
!# Number of modules:          2
!#

set spantree priority 4096

set arp-tx-interval 0

set logging server 149.49.38.22

set logging server condition all Informational 149.49.38.22

set logging file enable

snmp-server informs retries 5 timeout 30

snmp-server group sammy v3 auth read sammy write sammy

snmp-server group sammy v3 priv read iso write iso

snmp-server group initial v3 noauth read iso write iso
notify iso

snmp-server view initial 1.3.6.1.4.1.1751.2.53.1.2.1.3.*
included

snmp-server host 1.3.4.5 traps v3 noauth initial config
generic eth-port-faults

sw-redundancy temperature cam-Change l3-fault lag-events
policy link-down-fault supply fan cascade security
...
```

```
...
set time client disable

set ip route 0.0.0.0 149.49.138.1

set logout 0

set vlan 2 name V2

set vlan 3 name V3

set port static-vlan 1/1 3

set port static-vlan 1/2 3

rmon history 1025 1025 interval 30 buckets 10 owner "SYSTEM
on console11"

rmon history 1026 1025 interval 1800 buckets 10 owner
"Administrator on console2"

set snmp retries 5

no ip http

set ppp authentication incoming chap

set ppp incoming timeout 10

set radius authentication enable

set radius authentication server 149.49.138.161 primary

set radius authentication server 149.49.77.235 secondary

set allowed managers ip add 1.1.11.1
```

show license

User level: privileged, supervisor.

Use the `show license` command to display the current licenses installed on the stack.

The syntax for this command is:

```
show license
```

Example:

```
P330-N>show license
Mod      Application      License Key      State  Feature Flag
-----
1        smon             0000 0000 0000 0000 0000 0000  licensed  1
```

show log

User level: privileged, supervisor.

Use the `show log` command to display an encrypted device's reset log.

ⓘ This command is for Avaya technical support use.

The syntax for this command is:

```
show log [mod_num]
```

Example:

```
P330-N>show log 1
MODULE 1, MESSAGE 01:
00000000 0 05002966 0205 0 0 0 0 0 0 0 0 0 0 0
MODULE 1, MESSAGE 02:
00000000 0 00004242 0205 0 0 0 0 0 0 0 0 0 0 0
MODULE 1, MESSAGE 03:
00000000 0 00002395 0205 0 0 0 0 0 0 0 0 0 0 0
```

show logging file condition

User level: user, privileged, supervisor

Use the `show logging file condition` command to display the condition and filtering of the log file.

The syntax for this command is:

show logging file condition

Example:

```
P330-N>show logging file condition

*****
Message logging configuration of FILE      sink ***
Sink Is Enabled
Sink default severity: none
```

show logging file content

User level: user, privileged, supervisor

Use the `show logging file content` command to display the contents of the log file.

The syntax for this command is:

```
show logging file content [<severity>] [{all|<application>}]  
[<number>] [<module number>]
```

severity	The minimum severity of the logging messages that are displayed. The severity is represented by an integer. Possible values are: <ul style="list-style-type: none">• 0 – Emergency• 1 – Alert• 2 – Critical• 3 – Error• 4 – Warning• 5 – Notification• 6 – Informational• 7 – Debugging
all	A keyword signifying that the filter applies to logging messages from all applications.

application	The application to which the filter applies. Possible values are: <ul style="list-style-type: none">• BOOT• SYSTEM• ROUTER• CONFIG• FILESYS• FAN• SUPPLY• SECURITY• CASCADE• QOS• SWITCHFABRIC• LAG• VLAN• SNMP• POLICY• CLI• STP• THRESHOLD• CONSOLE
number	The number of messages to display. If no number is specified, all messages are displayed.
module	The number of the module from which the displayed messages originated. If no module is specified, messages from all modules are displayed.

Example:

```
P330-N>show logging file content 7 all
1 > 08/04/2003,15:43:36:CLI-Notification: root: set logging
file condition all 7
```

show logging server condition

User level: user, privileged, supervisor

Use the `show logging server condition` command to display the condition and filtering of logging to the Syslog server.

The syntax for this command is:

show logging server condition <ip-address>

ip-address The IP address of the Syslog server. If no IP address is specified, the condition and filtering of logging to all configured Syslog servers is displayed.

Example:

```
P330-N>show logging server condition 149.49.38.22

*****
Message logging configuration of SYSLOG   sink ***
Sink Is Enabled
Sink default severity: Warning

Server name: 149.49.38.22
Server facility: local7
Server access level: read-write
```


show logging session condition

User level: user, privileged, supervisor

Use the `show logging session condition` command to display the condition and filtering of logging in the current CLI session.

The syntax for this command is:

show logging session condition

Example:

```
P330-N>show logging session condition

*****
Message logging configuration of SESSION sink ***

Sink Is Enabled
Sink default severity: Error

Facility                ! Severity Override
-----
SUPPLY                  ! Warning
Session source ip: 135.64.102.224
```

show logout

User level: user, privileged, supervisor

Use the `show logout` command to display the amount of time the CLI remains idle before timing out in minutes.

If the result is 0, there is no timeout limit. The default is 15 minutes.

The syntax for this command is:

`show logout`

Example:

```
P330-N>show logout
CLI timeout is 10 minutes
```

show mac-aging

User level: user, privileged, supervisor

① This command is available on P330-ML-ML switches only.

Use the `show mac-aging` command to display the current status of the MAC aging function.

The syntax for this command is:

```
show mac-aging
```

Example:

```
P330-N>show mac-aging
mac aging application is disabled
```

show mac-aging-time

User level: user, privileged, supervisor

Use the `show mac-aging-time` command to display the MAC aging time in minutes.

The syntax for this command is:

```
show mac-aging-time
```

Example:

```
P330-N>show mac-aging-time
MAC aging time is 5 (min.)
```

- ① The displayed value is the aging time lower limit. The actual aging time can be up to 2 minutes longer.

show module

User level: user, privileged, supervisor

Use the `show module` command to display switch status and information. For each switch with an expansion sub-module installed, both switch and expansion sub-module type and information are shown.

The syntax for this command is:

```
show module [<mod_num>]
```

`mod_num` (Optional) Number of the switch/expansion sub-module. If you do not specify a number, all switches/expansion sub-modules are shown.

Example:

```
P330-N>show module
Mod      Type           C/S      S/N      Statuses
-----
 1  P333T          1.0      4144162  PS:OK Fans:OK Mode:Layer2
   X330GT2       2.0
   P330-MLSTK    2.0      Conn-Up:Fail Conn-Down:Ok
   BUPS          BUPS:Not Prsnt Fans:None Type:None

 2  P333T-PWR     3.0      4455428  PS:OK Fans:OK Mode:Layer2
   No Expansion Not Present
   P330-MLSTK    2.2      Conn-Up:Ok Conn-Down:Ok
   BUPS          BUPS:Not Prsnt Fans:None Type:None
```

Output Fields

Mod	Switch number
Type	Switch/Expansion module type
C/S	Hardware Configuration Symbol of the switch/expansion module
S/N	Serial number of the switch
Status	Status of the switch (and expansion module)

show module-identity

User level: user, privileged, supervisor

Use the `show module-identity` command to display the switch identity required for acquiring a license.

The syntax for this command is:

```
show module-identity [module]
```

Example:

```
P330-N>show module-identity
Mod      Module Identity
-----
 1      1234567
 2      4144162
```

show port

User level: user, privileged, supervisor

Use the `show port` command to display port status.

The syntax for this command is:

```
show port [<mod_num>[/port_num]]
```

mod_num
(Optional) Number of the switch. If you do not specify a number, the ports on all the switches are shown.

port_num
(Optional) Number of the port on the module (can be a virtual LAG port number). If you do not specify a number, all the ports on the switch are shown.

You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example: to display the status for port 4 on switch 3

P330-N> show port 3/4								
Port	Name	Status	Vlan	Level	Neg	Dup.	Spd.	Type
3/4	Gregory	no link	1	0	enable	half	10M	10/100BaseTx Port

Show Port Output Fields

Field	Description
Port	Switch and port number
Name	Name of port
Status	Status of the port (connected, no link, disabled)
Vlan	VLAN ID of the port
Level	Priority level of the port (0-7)
Neg	The autonegotiation status of the port (enabled, disabled)
Dup	Duplex setting for the port (full, half)
Speed	Speed setting for the port (10Mbps, 100Mbps, 1000Mbps)
Type	Port type, for example: <ul style="list-style-type: none"> 10/100Base-Tx, 1000Base-SX Port, Link Aggregation Group of 10/100Base-T ports

show port auto-negotiation-flowcontrol-advertisement

User level: privileged, supervisor.

Use the `show port auto-negotiation-flowcontrol-advertisement` command to display the flowcontrol advertisement for a Gigabit port used to perform auto-negotiation.

The syntax for this command is:

```
set auto-negotiation-flowcontrol-advertisement
[mod_num/port_num]
```

`mod_num` Number of the switch
(optional)

`port_num` Number of the port
(optional)

Example:

```
P330-N>show port auto-negotiation-flowcontrol-
advertisement

Port 1/1  advertises no flow control capabilities.
Port 1/2  advertises no flow control capabilities.
Port 1/3  advertises no flow control capabilities.
```

show port channel

User level: user, privileged, supervisor

Use the `show port channel` command to display Link Aggregation Group (LAG) information for a specific switch or port.

The syntax for this command is:

```
show port channel [<mod_num>[/<port_num>]] [info]
```

`mod_num` Number of the switch. If you do not specify a number, the
(Optional) modules on all the switches are shown.

`port_num` Number of the port on the switch. If you do not specify a
(Optional) number, all the ports on the switch are shown.
You can also specify a range of ports separated by a dash, for
example, 4/5-13 for ports 5 to 13 on switch 4.

`info` (Optional) Display port information

Example:

```
P330-N>show port channel
Port      Channel Status  Channel Name      Channel Id
-----
 1/1      on      MEIR              1/101
 1/2      on      MEIR              1/101
 1/3      off
 1/4      off
 1/5      on      my-channel        1/102
 1/6      on      my-channel        1/102
 1/7      off
 1/8      on      my-channel        1/102
P330-N>show port channel 3/3 info
Port      Speed Duplex  Vlan  Port      Trunk      Vlan
          Speed Duplex  Vlan  Priority  status     Binding
-----
 1/1      10    half    1      0         off        static
```

show port classification

User level: user, privileged, supervisor

Use the `show port classification` command to display a port's classification.

The syntax for this command is:

```
show port classification [module/[port]]
```

module	Number of the switch. If you do not specify a number, the ports on all the switches are shown.
port (Optional)	Number of the port on the module. If you do not specify a number, all the ports on the module are shown. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.

Example:

```
P330-N>show port classification 4/8
Port   Port Classification
-----
4/8    regular

P330-N>show port classification 4/9
Port   Port Classification
-----
4/9    valuable
```

show port dot1x

User level: user, privileged, supervisor

Use the `show port dot1x` command to display all the configurable values associated with the authenticator port access entity (PAE) and backend authenticator.

The syntax for this command is:

```
show dot1x [mod] / [port]
```

mod Number of the module.
(Optional)

port Number of the port on the module, or range of ports.
(Optional)

Example:

```
P330-N>show port dot1x 3/3
```

Port Number	Auth State	BEnd State	Port Control	Port Status	Re Auth	Quiet Priod	ReAuth Priod	Server Tmeout	Supp Tmeout	Tx Priod	Max Req
1/3	Init	Init	Auto	Unauth	Disa	60	3600	30	30	30	2

Port Number

Number of the module/port on the module.

Auth State

The Port Access Entity state. Possible states include:

- Initialize
- Disconnected
- Connecting
- Authenticating
- Authenticated
- Aborting
- Held
- ForceAuth
- ForceUnauth

BEnd Stat	<p>The current state of the Backend Authentication state machine. Possible states include:</p> <ul style="list-style-type: none">• Request• Response• Success• Fail• Timeout• Idle• Init
Port Control	<p>Port control type. Valid values include:</p> <ul style="list-style-type: none">• force-authorized• force-unauthorized• auto.
Port Status	<p>The current value of the controlled port status. Possible states include:</p> <ul style="list-style-type: none">• Authorized• Unauthorized
Re Auth	<p>The state of reauthentication on the port. Possible states include:</p> <ul style="list-style-type: none">• Enabled - The port connection is reauthenticated after the reAuthPeriod.• Disabled - The port connection is not reauthenticated. The reAuthPeriod is ignored.
Quiet Period	<p>The amount of time, in seconds, between sending authentication requests.</p>
ReAuth Period	<p>The time, in seconds, after which the port connection should be reauthenticated.</p>
Server Tmout	<p>The amount of time, in seconds, the P330-ML waits for a response from the RADIUS server.</p>
Supp Tmeout	<p>The amount of time, in seconds, before resending authentication requests.</p>
Tx Priod	<p>The amount of time, in seconds, in which an authentication request must be answered.</p>

Max Req

The maximum number of times a request for authentication is sent before timing out.

show port dot1x statistics*User level: user, privileged, supervisor*Use the `show port dot1x statistics` command to display all the port dot1x statistics.

The syntax for this command is:

`show dot1x statistics [mod]/[port]`

`mod` Number of the module.
(Optional)

`port` Number of the port on the module, or range of ports.
(Optional)

Example:

```
P330-N>show port statistics 1/1
```

Port	Tx_Req/Id	Tx_Req	Tx_Total	Rx_Start	Rx_Logff	Rx_Resp/Id	Rx_Resp
1/1	2	5	0	0	0	0	0
Port	Rx_Invalid	Rx_Len_Err	Rx_Total	Last_Rx_Frm_Ver	Last_Rx_Frm_Src_Mac		
1/1	0	0	0	0	1d-80-00-00-00-00		

show port edge state

User level: user, privileged, supervisor

Use the `show port edge state` command to show a port's edge admin and operational RSTP state.

- ① A port can be set to admin state of edge port, but if a BPDU is received on this port the oper state is changed to non-edge state.

The syntax for this command is:

```
show port edge state <module/port>
```

module/ Port identifier
port

Example:

```
P330-N>show port edge state
Port      admin state      oper state
-----  -
1/1      edge-port        edge-port
1/2      non-edge-port    non-edge-port
```

show port flowcontrol

User level: user, privileged, supervisor

Use the `show port flowcontrol` command to display per-port status information related to flow control.

The syntax for this command is:

```
show port flowcontrol [<mod_num>[/<port_num>]]
```

module Number of the switch . If you do not specify a number, all (Optional) switches are shown.

port Number of the port on the switch. If you do not specify a (Optional) number, all ports on the specified switch are shown.

Example:

```
P330-N>show port flowcontrol 3/4
Port      Send-Flowcontrol  Receive-Flowcontrol
          Admin Oper      Admin Oper
-----  -
3/4      off   off          off   off
```

Output Fields

Field	Description
Port	Module and port number
Send-Flowcontrol-Admin	Send flow-control administration. Possible settings: <ul style="list-style-type: none">• ON indicates that the local port is allowed to send flow control frames to the far end.• OFF indicates that the local port is <i>not</i> allowed to send flow control frames to the far end.
Send-Flowcontrol-Oper	Send flow-control operation mode. Possible modes: <ul style="list-style-type: none">• ON indicates that the local port will send flow control frames to the far end.• OFF indicates that the local port will <i>not</i> send flow control frames to the far end.
Receive-Flowcontrol-Admin	Receive flow-control administration. Possible settings: <ul style="list-style-type: none">• ON indicates that the local port will act upon flow control indications if received from the far end.• OFF indicates that the local port will discard flow control frames if received from the far end.
Receive-Flowcontrol-Oper	Receive flow-control operation mode. Possible modes: <ul style="list-style-type: none">• ON indicates that the local port will act upon flow control indications received from the far end.• OFF indicates that the local port will discard flow control frames received from the far end.

show port mirror

User level: user, privileged, supervisor

Use the show port mirror command to display mirroring information for the stack.

The syntax for this command is:

```
show port mirror
```

Example:

```
P330-N>show port mirror
port mirroring
-----
Mirroring both Rx and Tx packets from port 3/2 to port 4/4
is enabled

P330-N>show port mirror
port mirroring
-----
No ports are mirrored
```

show port point-to-point status

User level: user, privileged, supervisor

Use the show port point-to-point status command to show the port's point-to-point admin and operational RSTP status.

The syntax for this command is:

```
show port point-to-point status <module/port>
```

```
module/  Port identifier
port
```

Example:

```
P330-N>show port point-to-point status
Port      point-to-point admin state  point-to-point oper state
-----  -
1/1      auto                       point to point connection
1/2      auto                       point to point connection
1/3      auto                       point to point connection
1/4      auto                       point to point connection
1/5      auto                       point to point connection
1/6      auto                       point to point connection
1/7      auto                       point to point connection
```

show port redundancy

User level: user, privileged, supervisor

Use the `show port redundancy` command to display information about the port redundancy schemes defined for the switch. The “status” column displays which of the two redundancy member ports is enabled currently.

The syntax for this command is:

```
show port redundancy
```

Example:

```
P330-N>show port redundancy
Redundancy Name      Primary Port      Secondary Port      Status
-----
gregory              3/48              3/47                secondary
reuven               3/46              3/45                secondary
meir                 3/1               3/2                 primary
arie                 3/34              3/33                secondary

Port Redundancy global state is enable
Minimum Time between Switchovers: 1
Switchback interval: 3
```

show port security

User level: user, privileged, supervisor

Use the `show port security` command to list the security mode of the ports of a switch or stack. When no port number is specified, this command displays all the secured ports in the stack.

The syntax for this command is:

```
show port security [<module>[/<port>]]
```

Example:

```
P330-N>show port security 1
Switch-level security mode disabled
Violation action is restrict and notify
Port      Status
-----
1/1       enabled
1/2       disabled
1/3       disabled
...
```

show port trap

User level: user, privileged, supervisor

Use the `show port trap` command to display information on SNMP generic link up/down traps sent for a specific port.

The syntax for this command is:

```
show port trap [<module>[/<port>]]
```

module (Optional)	Number of the switches. If you do not specify a number, the ports on all the switches are shown.
port (Optional)	Number of the port on the switch. If you do not specify a number, all the ports on the switch are shown. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example:

```
P330-N>show port trap 4/1
Port 4/1 up/down trap is disabled
```

show port vlan-binding-mode

User level: user, privileged, supervisor

Use the `show port-vlan-binding` command to display port vlan binding mode information.

The syntax for this command is:

```
show port vlan-binding-mode [module[/port]]
```

module	Number of the switch. If you do not specify a number, the ports on all the switches are shown.
port (Optional)	Number of the port on the switch. If you do not specify a number, all the ports on the switch are shown. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on switch 4.

Example:

```
P330-N>show port vlan-binding-mode
port 2/1 is statically bound
port 2/2 is statically bound
port 2/3 is statically bound
port 2/4 is statically bound
port 2/5 is statically bound
port 2/6 is statically bound
port 2/7 is statically bound
port 2/8 is statically bound
port 2/9 is statically bound
port 2/10 is statically bound
```

Show powerinline

User level: user, privileged, supervisor

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `show powerinline` command to display the current status of the PD inline power on all ports.

The syntax of this command is:

```
show powerinline <mod_number [/<port_number>]>
```


Example:

```
P330-ML-2> show powerinline 3

External power Supply is 400Watts.
External power supply is active.

Port                Inline          Power          Powering
                   Operational    Allocated      Priority
                   Status        Class
-----            -
3/1                 on             0              Low
3/2                 on             0              Low
3/3                 on             0              High
3/4                 off            0              High
...
```

Example:

```
P330-ML-2> show powerinline 2/1

External power Supply is 400Watts.
External power supply is active.

Port                Inline          Power          Powering
                   Operational    Allocated      Priority
                   Status        Class
-----            -
2/1                 off            0              Low
```

show powerinline image version

User level: user, privileged, supervisor

- ① This command applies to P333T-PWR switches only and is used by P330-ML-ML switches to control P333T-PWR modules in the stack.

Use the `show powerinline image version` command to display the current

image version of P333T-PWR switches in the stack or a specific switch.

The syntax of this command is:

```
show powerinline image version [<module-number>]
```

If you do not specify a number, then the software version for all the P333T-PWR switches is shown.

module-number	Number of the module for which you want to display the current powerline image version
---------------	--

Example:

```
P330-ML-2> show powerinline image version
Mod                Image Version
---                -
1                  1.2.9
4                  1.2.9
5                  1.2.9
```

Example:

```
P330-ML-2> show powerinline 3
Mod                Image Version
---                -
3                  1.2.9
```

show ppp authentication

User level: user, privileged, supervisor

Use the `show ppp authentication` command to display the authentication method used for PPP sessions.

The syntax for this command is:

```
show ppp authentication
```

Example:

```
P330-N>show ppp authentication

PPP Authentication Parameters:
-----
Incoming:                CHAP
```

show ppp baud-rate

User level: user, privileged, supervisor

Use the `show ppp baud-rate` command to display the ppp baud-rate.

The syntax for this command is:

```
show ppp baud-rate
```

Example:

```
P330-N>show ppp baud-rate  
PPP baud rate is 38400
```

show ppp configuration

User level: user, privileged, supervisor

Use the `show ppp configuration` command to display the ppp configuration.

The syntax for this command is:

```
show ppp configuration
```

Example:

```
P330-N>show ppp configuration  
PPP baud rate is 38400  
PPP incoming timeout is 15 minutes  
PPP Authentication Parameters:  
-----  
Incoming:          None
```

show ppp incoming timeout

User level: user, privileged, supervisor

Use this `show ppp incoming timeout` command to display the amount of time in minutes that a PPP session can remain idle before being automatically disconnected.

The syntax for this command is:

```
show ppp incoming timeout
```

Example:

```
P330-N>show ppp incoming timeout  
PPP incoming timeout is 15 minutes
```

show ppp session

User level: user, privileged, supervisor

Use the `show ppp session` command to display PPP parameters and statistics of an active PPP session.

The syntax for this command is:

```
show ppp session
```

Example:

```
P330-N>show ppp session
```

show protocol

User level: user, privileged, supervisor

Use the `show protocol` command to display the current state of allowed protocols on the switch.

The syntax for this command is:

```
show protocol
```

Example:

```
P330-N>show protocol  
Protocols           Status  
-----           -  
SSH                 ON  
TELNET-CLIENT      OFF  
SNMPv1              OFF  
SNMPv3              ON  
TELNET              ON  
HTTP                OFF  
ICMP redirect       OFF  
recovery-password   ON
```

show queuing scheme

User level: user, privileged, supervisor

① This command is available on P330-ML-ML switches only

Use the `show queuing scheme` command to display the current queuing scheme settings.

① If this command is to be implemented on a P330-ML-ML switch other than the stack master, a session should be opened to the relevant switch.

The syntax for this command is:

```
show queuing scheme
```

Example:

```
P330-N>show queuing scheme
Module Queuing Scheme

-----

1    Default

2    Wrr 10:1
```

show radius authentication

User level: user, privileged, supervisor

Use the `show radius authentication` command to display all RADIUS authentication configurations.

The syntax for this command is:

```
show radius authentication
```

Example:

```
P330-N>show radius authentication
RADIUS authentication parameters:
-----
Mode:                               Enabled
Primary-server:                      192.168.42.252
Secondary-server:                    192.168.48.134
Retry-number:                         4
Retry-time:                           5
UDP-port:                             1645
Shared-secret:                        sodot
```

show rmon alarm

User level: user, privileged, supervisor

Use the `show rmon alarm` command to display the parameters set for a specific alarm entry that was set using the `rmon alarm` command on or using the P330-ML Manager.

The syntax for this command is:

```
show rmon alarm [<Alarm Index>]
```

Alarm Index	History index defined using <code>rmon alarm</code> command or the P330-ML Manager.
-------------	---

Example:

```
P330-N>show rmon alarm 1026

alarm

alarm 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 60 seconds
Taking delta samples, last value was 1712
Rising threshold is 10000, assigned to event # 1054
Falling threshold is 10, assigned to event # 1054
On startup enable rising or_falling alarms.
```

show rmon event

User level: user, privileged, supervisor

Use the `show rmon event` command to show the parameters of an Event entry defined by the `rmon event` command or using the P330-ML Manager.

The syntax for this command is:

```
show rmon event [<Event Index>]
```

Alarm Index	History index defined using <code>rmon event</code> command or the P330-ML Manager
-------------	--

Example:

```
P330-N>show rmon event 1026

event

Event 1054 is active, owned by amir
Description is event for monitoring amir's co
Event firing causes log and trap to community public,last
fired 0:0:0
```

show rmon history

User level: user, privileged, supervisor

Use the `show rmon history` command to display the most recent RMON history log for a given History Index. The history index is defined using the `rmon history` command or using an RMON management tool.

The syntax for this command is:

```
show rmon history [<History Index>]
```

History Index	History index defined using <code>rmon history</code> command or RMON management tool
---------------	---

Example:

```
P330-N>show rmon history 1026
history
Entry 1026 is active, owned by amir
Monitors ifEntry.1.1026 every 30 seconds
Requested # of time intervals, ie buckets, is 20
Granted # of time intervals, ie buckets, is 20
Sample # 1 began measuring at 2:53:9
Received 62545 octets, 642 packets,
391 broadcast and 145 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

show rmon statistics

User level: user, privileged, supervisor

Use the `show rmon statistics` command to show the Received Packet RMON statistics counters for a certain interface number according to the MIB-2 interface table numbering scheme.

The syntax for this command is:

```
show rmon statistics <module/port>
```

module/port Range of ports

Example:

```
P330-N>show rmon statistics
Statistics for switch is active,owned by Monitor
Monitors ifEntry.1.1026 which has
Received 26375085 octets, 222536 packets,
154821 broadcast and 53909 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
1 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
# of packets received of length (in octets):
64:94530, 65-127:85124, 128-255:25896,
256-511:10440, 512-1023:6057, 1024-1518:489
```

show secure current

User level: user, privileged, supervisor

Use the `show secure current` command to list the IP addresses of managers currently connected to the switch.

The syntax for this command is:

```
show secure current
```

Example:

```
P330-N# show secure current
  IP Address                               Time Since Last Request(In Sec)
  -----                               -
  135.64.100.205                            7
  149.49.77.13                              13
  149.49.77.7                               2
```

show secure mac

User level: user, privileged, supervisor

Use the `show secure mac` command to display the secure MAC address defined for a secured port.

The syntax for this command is:

```
show secure mac [<mod-num>/<port-num>]
```

`mod-num`

Module where the secured port is located

port-num Secured port number

Example:

```
P330-N# show secure mac port 1/7
Port      Secure-Src-Addrs
-----
1/7       00-40-0d-9b-9d-00
          00-40-0d-98-61-2e
          00-40-0d-8a-a3-23
```

show security mode

User level: user, privileged, supervisor

Use the `show security mode` command to display the status of the MAC security feature.

The syntax for this command is:

show security mode

Example:

```
P330-N# show security mode

Switch-level security mode disabled
Violation action is restrict and notify
```

show snmp

User level: user, privileged, supervisor

Use the `show snmp` command to display SNMP information.

The syntax for this command is:

show snmp

Example:

```
P330-N>show snmp
```

```
Authentication trap enabled
```

Community-Access	Community-String	
-----	-----	
read-only	public	
read-write	public	
trap	meir	

Trap-Rec-Address	Status	Traps Configured
-----	-----	-----
135.64.100.73	Enabled	config fault traffic_threshold module_De-Enrollment module_Enrollment delete_SW_redundancy_entry create_SW_redundancy_entry temperature_warning general_threshold cam_change duplicate_ip ip_vlan_violation link_aggregation_connection_fault link_aggregation_connection_return link_aggregation_partial_fault link_aggregation_partial_return link_aggregation_auto_neg_fault link_aggregation_auto_neg_fault_return delete_lag create_new_lag active_policy_list_change policy_access_control_violation PSU_module_fault PSU_module_fault_return BUPS_module_fault BUPS_module_fault_return BUPS_fans_module_fault BUPS_fans_module_fault_return fans_module_fault fans_module_fault_return cascade_up_connection_fault Cascade_up_connection_fault_return Cascade_down_connection_fault_return Cascade_down_connection_fault

```
SNMPv3 Notifications Status
```

```
-----  
Traps: Enabled  
Informs: Enabled                   Retries: 5    Timeout: 30 seconds
```

SNMP-Rec-Address	Model	Level	Notification	Trap/Inform	User name
135.64.100.73 UDP port: 162	v1	noauth	config sw-redundancy temperature cam-Change supply l3-fault link-down-fault lag-events fan cascade policy eth-port-faults security generic	trap	WriteCommN
149.64.100.73 UDP port: 162	v3	noauth	config sw-redundancy temperature cam-Change supply l3-fault link-down-fault lag-events fan cascade policy eth-port-faults security generic	trap	initial

show snmp engineID

User level: supervisor

Use the `show snmp engineID` command to display SNMP engine information.

The syntax for this command is:

show snmp engineID

Example:

```
P330-N>show snmp engineID
EngineId: 1a:e9:00:00:01:95:31:8a:9d
EngineBoots: 3
```

Output fields:

Field	Description
EngineId	The SNMP engine ID.
EngineBoots	The number of times the SNMP engine has been started or reinitialized.

show snmp group

User level: supervisor

Use the `show snmp group` command to display SNMP groups.

The syntax for this command is:

show snmp group [`<group-name>`]

group-name (optional)	The name of a group to display. If no group is specified, all groups are displayed.
--------------------------	---

Example:

```
P330-N>show snmp group

Group Name: initial
Security Model: v3
Security Level: noauth
Read View: iso
Write View: iso
Notify View: iso
Status: active

Group Name: ReadCommG
Security Model: v1
Security Level: noauth
Read View: snmpv1View
Write View:
Notify View: snmpv1View
Status: active

Group Name: ReadCommG
Security Model: v2c
Security Level: noauth
Read View: snmpv1View
Write View:
Notify View: snmpv1View
Status: active
...
```

show snmp retries

User level: user, privileged, supervisor

Use the `show snmp retries` command to display the number of retries initiated by the P330-ML Embedded Web Manager when it tries to send SNMP messages to the device.

The syntax for this command is:

show snmp retries

Example:

```
P330-N>show snmp retries
the SNMP Retries Number is 3
```

show snmp timeout

User level: user, privileged, supervisor

Use the `show snmp timeout` command to display the default SNMP timeout in seconds. The SNMP timeout is only for the Avaya P330-ML Embedded Web Manager.

Tip: This command is useful for access using the Device Manager.

The syntax for this command is:

show snmp timeout

Example:

```
P330-N>show snmp timeout
the SNMP Timeout is 2000
```

show snmp user

User level: supervisor

Use then `show snmp user` command to display command to display SNMP

information for a specific user.

The syntax for this command is:

show snmp user [<user>]

user	Name of the user. If no user is specified, SNMP information for
(Optional)	all users is displayed.

Example:

```
P330-N>show snmp user initial

EngineId: 1a:e9:00:00:01:95:31:4b:64   (local)
User Name: initial
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
```

show snmp userToGroup

User level: supervisor

Use then `show snmp userToGroup` command to display the assignment of users to SNMPv3 groups.

The syntax for this command is:

show snmp userToGroup

Example:

```
P330-N>show snmp userToGroup
```

```
Security Model: v1
Security Name: ReadCommN
Group Name: ReadCommG
```

```
Security Model: v1
Security Name: WriteCommN
Group Name: WriteCommG
```

```
Security Model: v2c
Security Name: ReadCommN
Group Name: ReadCommG
```

```
Security Model: v2c
Security Name: WriteCommN
Group Name: WriteCommG
```

```
Security Model: v3
Security Name: initial
Group Name: initial
```

show snmp view

User level: supervisor

Use the `show snmp view` command to display SNMP view configurations. If no view name is provided, the configuration of all SNMP views is displayed.

The syntax for this command is:

```
show snmp view [<viewname>]
```

<code>viewname</code>	Name of the view. If you do not specify a view, the
(Optional)	configuration of all SNMP views is displayed.

Example:

```
P330-N>show snmp view snmpv1View
```

```
View Name: snmpv1View  
Subtree Oid: 1  
Subtree Mask:  
View Type: include  
Storage Type: nonVolatile  
Status: active
```

```
View Name: snmpv1View  
Subtree Oid: 1.3.6.1.6  
Subtree Mask:  
View Type: exclude  
Storage Type: nonVolatile  
Status: active
```

Output fields:

Field	Description
View Name	The name of the view.
Subtree Oid	The name of a MIB subtree in OID format or as a textname mapped to a valid OID.
Subtree Mask	The subtree mask. This can be all ones, all zeros, or a combination of both.
View Type	Status of whether the MIB subtree is included or excluded.
Storage Type	The type of storage used to store the view configuration. Possible values are: <ul style="list-style-type: none"> • nonVolatile – The configuration is saved in non-volatile memory and is retained after the stack is reset. • Volatile – The configuration is saved in volatile memory and is not retained when the stack is reset.

show spantree

User level: user, privileged, supervisor

Use then show `spantree` command to display spanning-tree information.

The syntax for this command is:

show spantree [`<mod_num>` [`/<port_num>`]]

<code>mod_num</code> (Optional)	Number of the switch. If you do not specify a number, all switches are shown.
<code>port</code> (Optional)	Number of the port on the switch. If you do not specify a number, all ports on the specified switch are shown.

Example:

```
P330-N>show spantree

Spanning tree state is enabled

Designated Root: 00-40-0d-8c-88-ff
Designated Root Priority: 32768
Designated Root Cost: 100
Designated Root Port: 1/7
Root Max Age: 20 Hello Time: 2
Root Forward Delay: 15

Bridge ID MAC ADDR: 00-40-0d-b9-89-ff
Bridge ID priority: 32768
Bridge Max Age: 20 Bridge Hello Time: 2
Bridge Forward Delay: 15 Tx Hold Count 3
Spanning Tree Version is rapid spanning tree
Spanning Tree Default Path Costs is according to common
spanning tree

Port      State          Cost      Priority
-----  -
4 /1     not-connected  19        128
4 /2     not-connected  19        128
4 /3     LAG-member    19        128
4 /4     LAG-member    19        128
4 /5     not-connected  19        128
4 /6     not-connected  19        128
4 /8     not-connected  19        128
4 /9     not-connected  19        128
4 /10    not-connected  19        128
4 /11    not-connected  19        128
```

Output fields:

Field	Description
Spanning tree	Status of whether Spanning-Tree Protocol is enabled or disabled
Designated Root	MAC address of the designated spanning-tree root bridge
Designated Root Priority	Priority of the designated root bridge
Designated Root Cost	Total path cost to reach the root
Designated Root Port	Port through which the root bridge can be reached (shown only on nonroot bridges)
Root Max Age	Amount of time a BPDU packet should be considered valid
Hello Time	Number of times the root bridge sends BPDUs
Root Forward Delay	This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state.
Bridge ID MAC ADDR	Bridge MAC address used in the sent BPDUs
Bridge ID Priority	Bridge priority
Bridge Max Age	The value that all bridges use for MaxAge when this bridge is acting as the root.
Bridge Hello Time	The value that all bridges use for HelloTime when this bridge is acting as the root.
Bridge Forward Delay	The value that all bridges use for ForwardDelay when this bridge is acting as the root.
Tx Hold Count	The value used by the Port Transmit state machine to limit the maximum transmission rate.
Soanning Tree Version	The version of Spanning Tree Protocol the bridge is currently running

Spanning Tree Default Path Costs	The version of the Spanning Tree default Path Costs that are to be used by this Bridge.
Port	Port number
State	Spanning-tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent)
Cost	Cost associated with the port
Priority	Priority associated with the port

show system

User level: user, privileged, supervisor

Use the `show system` command to display the up time, system name, location, and contact person.

The syntax for this command is:

show system

Example:

```
Router-N> show system
Uptime d,h:m:s
-----
0,2:40:55

System Name           System Location           System Contact
-----
P332_version-3.0.5    Alpha LAB                  Ygdal Naouri

Switch MAC address
-----
00 40 0d 8a 04 b4
```

show tftp download software status

User level: user, privileged, supervisor

Use the `show tftp download software status` commands to display the status of the current TFTP Device Manager S/W (Embedded Web) download process into the device.

The syntax for this command is:

show tftp download software status [`<mod_num>`]

Example:

```
P330-N>show tftp download software status

Module #1

=====

Module           : 1
Source file      : p340_4_0_4.web
Destination file : EW_Archive
Host             : 149.49.100.51
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded : 1860987

=====
```

show time

User level: user, privileged, supervisor

Use the `show time` command to display the current P330-ML time and timezone.

The syntax for this command is:

show time

Example:

```
P330-N>show time  
10:32:34 27 JAN 2000 GMT
```

show time parameters

User level: user, privileged, supervisor

Use the `show time parameters` command to display the time status and parameters.

The syntax for this command is:

show time parameters

Example:

```
P330-N>show time parameters  
Client status: Enabled  
Current time : L:00:57:19 01 JAN 1970 GMT  
Timezone set to 'GMT', offset from UTC is 0 hours  
Time-Server : 0.0.0.0 (I.e. broadcast address)  
Time acquired from Time-Server: 0.0.0.0  
Time protocol set to : TIME protocol
```

show timeout

User level: user, privileged, supervisor

Use the `show timeout` command to display the amount of time the CLI can remain idle before timing out in minutes. If the result is 0, there is no timeout limit. The default is 15 minutes.

The syntax for this command is:

show timeout

Example:

```
P330-N>show timeout  
CLI timeout is 10 minutes
```

show timezone

User level: user, privileged, supervisor

Use the `show timezone` command to display the current P330-ML time zone.

The syntax for this command is:

show timezone

Example:

```
P330-N>show timezone  
Timezone set to 'GMT', offset from UTC is 0 hours
```

show trunk

User level: user, privileged, supervisor

Use the `show trunk` command to display VLAN tagging information for the switch or a specified module or port.

The syntax for this command is:

show trunk [`<mod_num>`[/`<port_num>`-`<port_num>`]]

<code>mod_num</code> (Optional)	Number of the switch. If you do not specify a number, all switches in the stack are shown.
<code>port_num</code> (Optional)	Number of the port on the switch. If you do not specify a number, all ports on the specificity switch are shown. You can specify a port range.

Example:

```

P330-N>show trunk 4/1-2
P330-ML-1(super)# show trunk 1/42-44

Port   Mode   Binding mode           Native vlan Vlans allowed on trunk
-----
1/42   off    bound to configured vlans   1         1-9,500

Port   Mode   Binding mode           Native vlan Vlans allowed on trunk
-----
1/43   off    statically bound         1         1,7-8

Port   Mode   Binding mode           Native vlan Vlans allowed on trunk
-----
1/44   dot1q bound to all vlans       500       1-3071

```

Output Fields:

Field	Description
Port	Switch and port number(s)
Mode	Tag status of the port (dot1q - dot1Q tagging mode, off - clear mode).
Binding mode	Binding mode of the port
Native VLAN	Number of the Port VLAN ID (the VLAN to which received untagged traffic will be assigned).

show upload status

User level: user, privileged, supervisor

Use the `show upload status` commands to display the status of the current configuration file copy process from the device.

The syntax for this command is:

show upload status [<mod_num>]

mod_num Number of the module. If you do not specify a number, upload statuses for all modules in the stack are shown.
(Optional)

Example:

```
Router-N> show upload status 1
Module           : 1
Source file      : stack-config
Destination file : c:\conf.cfg
Host             : 149.49.36.200
Running state    : Executing
Failure display  : (null)
Last warning     : No-warning
```

show username

User level: supervisor

Use the `show username` command to display the local user accounts.

The syntax for this command is:

show username

Example:

```
P330-1(super)# show username
```

User account	password	access-type
root	*****	admin
gkohll	*****	read-only
readwrite	*****	read-write

show utilization

User level: privileged, supervisor.

Use the `show utilization` command to display CPU utilization statistics for modules in the stack.

The syntax for this command is:

show utilization <module-number>

module-number The module for which to display utilization statistics. If no module is specified, utilization statistics for all modules is displayed.

Example:

```
P330-1(super)# show utilization
```

Mod	CPU 5sec	CPU 60sec	RAM used(%)	RAM Total (Kb)
---	-----	-----	-----	-----
1	Appl. Disabled		67%	23354 Kb

show vlan

User level: user, privileged, supervisor

Use the `show vlan` command to display the VLANs configured in the stack or switch or the ports bound to a specified VLAN.

The syntax for this command is:

```
show vlan { <vlan-number> | <vlan-name> }
```

vlan-number The VLAN ID for which to display bound ports.

vlan-name The VLAN name for which to display bound ports.

Examples:

```
P330-N>show vlan
```

```
VLAN ID Vlan-name
```

```
-----
1         v1
5         V5
10        V10
15        V15
20        V20
25        V25
```

```
P330-N>show vlan 7
```

```
VLAN ID Vlan-name
```

```
-----
7         V7
```

```
Switch Ports currently bound to this vlan:
```

```
In module 1 : 9 42 43 44
```

```
Switch Ports statically bound to this vlan:
```

```
In module 1 : 43
```

Output Fields:

Field	Description
VLAN ID	The VLAN ID.
Vlan-name	The VLAN name.
Switch Ports currently bound to this vlan	Switch ports that have this VLAN as their PVID, are statically bound to this VLAN, or configured as bind-to-all or bind-to-configure.
Switch Ports statically bound to this vlan	Switch ports that are statically bound to this VLAN.

show web aux-files-url

User level: user, privileged, supervisor

Displays the URL/directory from where the switch can access the Device Manager auxiliary files (for example help files).

The syntax for this command is:

```
show web aux-files-url
```

Example:

```
P330-N>show web aux-files-url
the web aux-files-url is 149.49.36.212/P330-MLtest
```

snmp-server community

User level: supervisor

Use the `snmp-server community` command to enable access to the switch using community names. Access using community names is enabled by default.

The syntax for this command is:

```
snmp-server community
```

Example:

```
P330-N>snmp-server community
Done!
```

snmp-server enable

User level: supervisor

Use the `snmp-server` `enable` command to enable SNMP Access to the switch.

The syntax for this command is:

snmp-server enable [volatile]

volatile (Optional) By default the activation of the `snmp-server` command is permanent and automatically stored in the non-volatile memory. The SNMP server is automatically launched after all restarts. If the `volatile` parameter is provided, then the SNMP service runs only until the stack is reset.

Example:

```
P330-N>snmp-server enable
Done!
```

snmp-server enable notifications

User level: supervisor

Use the `snmp-server enable notifications` command to enable sending all Simple Network Management Protocol (SNMP) notifications (traps and informs).

The syntax for this command is:

snmp-server enable notifications

Example:

```
P330-N>snmp-server enable notifications
Done!
```

snmp-server engineID

User level: supervisor

Use the `snmp-server engineID` command to change the SNMP Engine ID. Only the default user can run this command.

The syntax for this command is:

snmp-server engineID <engineID>

engineID A 5 - 32 byte string represented as hexadecimal numbers separated by the colon character.
For example, 00:00:00:81:0a:fe:ff:12:97:33:45:12.

Example:

```
P330-N>snmp-server engineID 1a:e9:00:00:01:95:31:8a:9d
P330-N>EngineID changed
P330-N>Done!
```

snmp-server group

User level: supervisor

Use the `snmp-server group` command to configure SNMPv3 groups.

The syntax for this command is:

snmp-server group <groupname> [**v1** | **v2c** | **v3** { **noauth** | **auth** | **priv** }] [**read** readview] [**write** writeview] [**notify** notifyview]

groupname	Variable that specifies the name of the SNMP group. The maximum length is 32 bytes.
v1, v2c, v3	The security model assigned to the group.
noauth, auth, priv	Keywords that specifies the type of authentication. <ul style="list-style-type: none">• noauth – No authentication required.• auth – Requires authentication with no encryption.• priv – Requires authentication with encryption.
read	Keyword that specifies a view for SNMP get requests. If this keyword is not included in the command, the group has no associated read view.
readview	The name of the view for SNMP get requests.
write	Keyword that specifies a view for SNMP set requests. If this keyword is not included in the command, the group has no associated write view.
writeview	The name of the view for SNMP set requests.

notify	Keyword that specifies a view for SNMP notifications. If this keyword is not included in the command, the group has no associated notify view.
<code>notifyview</code>	The name of the view for SNMP notifications.

Example:

```
P330-N>snmp-server group newgroupG v3 noauth read
4I2readonlyV3 write 32initialView notify TrapSender4V
Done!
```

snmp-server host

User level: supervisor

Use the `snmp-server host` command to specify the recipient of the notification operations and filter traps to that station. This command provides maximum flexibility. For each notification group you can define one of four states — disabled, generated as a trap, generated as inform, or generated as both inform and trap.

The syntax for this command is:

```
snmp-server host <host-addr> {traps | informs} {{v1 | v2c}
<community-name>} | {v3 {auth | noauth | priv}
<security-name>} [udp-port <port>] [<notification-type-list>]
```

<code>host-addr</code>	Specifies the address (or host name) of the notification recipient agent. The maximum length is 32 bytes.
traps, informs	Keyword that specifies whether to use traps or informs for notification to the specified recipient.
v1, v2c, v3	The security model assigned to the host.
<code>community-</code> <code>name</code>	The SNMPv1/SNMPv2c community string to use for notifications.
noauth, auth, priv	Keywords that specifies the type of authentication for SNMPv3 hosts. <ul style="list-style-type: none"> • noauth – No authentication required. • auth – Requires authentication with no encryption. • priv – Requires authentication with encryption.
<code>security-</code> <code>name</code>	The SNMPv3 user name to use for notifications.

udp-port (Optional)	Keyword that specifies that a specific UDP port on the target host should be used when sending notifications to the host. The default UDP port is 162.
<code>port</code>	The UDP port on the target host to which notifications are sent.
<code>notification</code> <code>-type-list</code> (Optional)	List of notification types. Each types combines related notifications. You can enable or disable notification generations on a per group basis. For example, the <code>swRedundancy</code> type groups new and delete software redundancy notifications. If no notification-type-list is specified, the default, all, is used. <ul style="list-style-type: none">• <code>all/*</code> – All traps• <code>generic</code> – Generic traps• <code>config</code> – Config change notifications• <code>eth-port-faults</code> – Ethernet port fault notifications• <code>sw-redundancy</code> – Software redundancy notifications• <code>temperature</code> – Temperature warning notifications• <code>cam-change</code> – Changes in CAM notifications• <code>l3-faults</code> – Layer 3 faults, including duplicate IP and VLAN violations• <code>lag-event</code> – Link aggregation faults and configuration changes• <code>policy</code> – Changes in policy notifications (for L3 devices)• <code>link-down-faults</code> – ITC proprietary link down notifications• <code>supply</code> – Power supply notifications (main and backup)• <code>fan</code> – FAN faults notifications (main and backup)• <code>cascade</code> – Cascade connection fault notifications. Note that the list of notification names is proprietary to ITC.

Example:

```
P330-N>snmp-server host 149.49.38.221 informs v3 noauth  
charlieBrown  
Done!
```

snmp-server informs

User level: supervisor

Use the `snmp-server informs` command to configure inform parameters.

The syntax for this command is:

```
snmp-server informs retries <retries-num> timeout <seconds>
```

retries-num Maximum number of times to resend an inform request.

seconds Number of seconds to wait for an acknowledgment before resending. The default is 3.

Example:

```
P330-N>snmp-server informs retries 5 timeout 30
Done!
```

snmp-server remote-user

User level: supervisor

Use the `snmp-server remote user` command to configure a remote-user as a target for SNMP notifications.

The syntax for this command is:

```
snmp-server remote-user <username> <engineID> <groupname>
{ v1 | v2c | v3 } [auth {md5 | sha} <auth-password>
[priv des56 <priv-password>]]
```

username Variable that specifies the name of the SNMP user. The maximum length is 32 bytes.

engineID The remote SNMP engineID. The SNMP engineID is a 12 byte string represented as hexadecimal numbers separated by the colon character.
For example, 00:00:00:81:0a:fe:ff:12:97:33:45:12.

groupname Variable that specifies the name of the SNMP group. The maximum length is 32 bytes.

v1, v2c, v3 The security model assigned to the user in user to group association.

auth
(Optional) A keyword signifying that an authentication password is required.

md5, sha Keyword that specifies authentication protocol, either HMAC-SHA-96 or MAC-MD5-96.

priv-
password The privacy password. Valid lengths are 8 - 64 characters.

priv des56 (Optional)	A keyword signifying that a privacy password is required.
auth- password	The authentication password. Valid lengths are 8 - 64 characters.

Example:

```
P330-N>snmp-server remote-user charles
22:00:00:01:6e:4a:32:22:01 2L2NotifyG3

Done!
```

snmp-server user

User level: supervisor

Use the `snmp-server user` command to configure a new SNMP user.

The syntax for this command is:

```
snmp-server user <username> <groupname> { v1 | v2c | v3 }
[auth {md5 | sha} <auth-password> [priv des56 <priv-
password>]]
```

username	Variable that specifies the name of the SNMP user. The maximum length is 32 bytes.
groupname	Variable that specifies the name of the SNMP group. The maximum length is 32 bytes.
v1, v2c, v3	The security model assigned to the user in user to group association.
auth (Optional)	A keyword signifying that an authentication password is required.
md5, sha	Keyword that specifies authentication protocol, either HMAC-SHA-96 or MAC-MD5-96.
priv- password	The privacy password. Valid lengths are 8 - 64 characters.
priv des56 (Optional)	A keyword signifying that a privacy password is required.
auth- password	The authentication password. Valid lengths are 8 - 64 characters.

Example:

```
P330-N>snmp-server user jimmyd v3AdminViewG v3 auth md5
Ar43*ffr20 priv des56 asdf$sWE4522
Done!
```

snmp-server view

User level: supervisor

Use the `snmp-server view` command to configure an SNMP MIB view. Use multiple iterations of the command to add or remove OIDs from the view.

The syntax for this command is:

```
snmp-server view <view-name> <oid-tree> {included | excluded}
```

<code>view-name</code>	Name of the view.
<code>oid-tree</code>	Object identifier (OID) of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4. To specify a subtree family, use the asterisk as a wildcard character. For example, 1.3.6.1.2.1.2.2.1.*.1 includes access to all elements of the first row in IfTable. Symbolic MIB object names are not supported.
included	Keyword specifying that the subtree specified by <code>oid-tree</code> is included in the view.
excluded	Keyword specifying that the subtree specified by <code>oid-tree</code> is excluded from the view.

Example:

```
P330-N>snmp-server view initial
1.3.6.1.4.1.1751.2.53.1.*.2.1.3 included
Done!
```

stack health

User level: privileged, supervisor.

Use the `stack health` command to test the integrity of stacking modules and cables.

① You can only run this command on a stack.

- ① The stack is reset once the command has been executed.
- ① You should not load the stack with traffic during this test.
- ① Please follow the instruction shown on the CLI screen, during the various stages of this test.

The syntax for this command is:

`stack health`

Example:

```
P330-N>stack health

TThis operation will eventually result in a Stack reset.
- do you want to continue (Y/N)? y

Start testing stack health....
This test will take a few minutes!!
The stack health test was completed successfully
```

sync time

User level: privileged, supervisor.

Use the `sync time` command to synchronize the time used by all modules in the switch.

The syntax for this command is:

sync time

Example:

```
P330-N# sync time
Time has been distributed.
```

tech

User level: supervisor

Use the `tech` command to enter tech mode. This command is reserved for service personnel use only.

telnet

User level: user, privileged, supervisor

Use the `telnet` command to open a Telnet session to a remote host.

The syntax for this command is:

```
telnet <ip-address> [<port-number>]
```

ip-address The IP address of the remote host.

port-number The port number over which to open the Telnet connection.

Example:

```
P330-N>telnet 149.22.38.127
```

terminal

User level: user, privileged, supervisor

Use the `terminal width` and `terminal length` commands to set the width and length of the terminal display in characters.

The syntax for this command is:

```
terminal {width|length} [<characters>]
```

Example:

```
Router-N> terminal width 80  
terminal width: 80
```

username

User level: supervisor

Adds a local user account.

- ① By default there is only a single user account, named 'root', with password 'root', which access the administrator level. You cannot delete this basic user account, nor can you modify its access level. You can modify its basic password.

The syntax for this command is:

```
username <name> password <passwd> access-type {read-only|read-write|admin}
```

name New user name (minimum four characters)

passwd User's password (minimum four characters)

access-type Access type definition - read only, read-write or administrator

Example:

```
P330-1(super)# username john password johnny access-type
read-write
User account added.

P330-1(super)# username root password secret access-type
read-write
ERROR: User account root has always an administrator access
type.

P330-1(super)# username root password secret access-type
admin
User account modified.
```

- ① If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

validate-group

User level: privileged, supervisor.

- ① This command applies to the P334T-ML only when it is in device mode "Layer2".

Use the `validate-group` command to verify that all the rules in a policy list are valid.

- ① If there is a configuration problem with a specific rule, or with a number of rules, detailed error messages will be given.

The syntax for this command is:

```
validate-group <policy-list-number>[quiet]
```

policy-list-number	A valid id number for the policy list currently defined for the switch
quiet	does not display error messages

Example:

```
P330-N# validate-group 101  
List 101 is valid-in-progress  
  
P330-N# validate-group 101  
List 101 is valid
```

- ① The validation process may take some time to complete.

Avaya P330-ML Layer 3 CLI Commands

This chapter provides all the Layer 3 CLI (Command Line Interface) commands, parameters, and their default values.

How the Layer 3 CLI is Organized

The commands that make up the Layer 3 CLI are organized alphabetically and according to context.

Router Configuration Contexts

You can either use the general Layer 3 commands available from the `Router(configure) #` prompt or you can enter one of two router configuration context modes:

Router interface context

Allows you to define parameters individually for each interface. To enter this context, type **interface** <interface_name>

The prompt changes to `Router-N(config-if:<interface_name>) #`

Router protocol context

Allows you to define parameters for a specific routing protocol (RIP, OSPF, and SRRP). To enter this context, type **router** <protocol_name>

The prompt changes to `Router-N(config router:<protocol_name>) #`

To exit these context modes, type the command **exit**.

Shortcuts to Commands by Context

Command descriptions are organized into the following contexts:

General Commands	Page 212
Interface context Commands	Page 274
Router RIP context Commands	Page 291
Router OSPF context Commands	Page 293
Router SRRP context Commands	Page 296

General Commands

arp

User level: privileged, supervisor.

- ① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `arp` command to add a permanent entry to the Address Resolution Protocol (ARP) cache.

Use the `no arp` command to remove an entry, either static entry or dynamically learned.

The syntax for this command is:

```
[no] arp <ip-address> <mac-address>
```

<code>ip-address</code>	IP address, in dotted decimal format, of the station
<code>mac-address</code>	MAC address of the local data link

Example:

To add a permanent entry for station 192.168.7.8 to the ARP cache:

```
Router-N(configure)# arp 192.168.7.8 00:40:0d:8c:2a:01
```

Example:

To remove an entry to the ARP cache for the station 192.168.13.76:

```
Router-N(configure)# no arp 192.168.13.76
```

arp timeout

User level: privileged, supervisor.

- ① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `arp timeout` command to set the amount of time that an entry remains in the ARP cache.

Use the `no arp timeout` command to restore the default value, 14,400.

The syntax for this command is:

```
[no] arp timeout <seconds>
```

seconds	The amount of time, in seconds, that an entry remains in the arp cache.
---------	---

Example:

To set the arp timeout to one hour:

```
Router-N(configure)# arp timeout 3600
```

To restore the default arp timeout:

```
Router-N(configure)# no arp timeout
```

clear arp-cache

User level: privileged, supervisor.

① If you are at the "privileged" level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `clear arp-cache` command to delete dynamic entries from the ARP cache and the IP route cache.

The syntax for this command is:

```
clear arp cache [<vlan>|<ip addr> [<mask>]]
```

vlan	VLAN string (up to 16 characters)
ip addr	IP address
mask	IP mask

Example:

```
Router-N(configure)# clear arp-cache  
Flushing all arp entries  
Flushed 100 ARP entries  
Done!
```

clear fragment

User level: privileged, supervisor.

Use the `clear fragment` command to restore fragment action database defaults and free all waiting fragments.

The syntax for this command is:

```
clear fragment
```

Example:

```
Router-N# clear fragment  
  
Done!
```

clear ip route

User level: privileged, supervisor.

Use the `clear ip route` command to delete one or all of the dynamic routing entries from the Routing Table (RIP only).

The syntax for this command is:

```
clear ip route * | <ip-addr> [<ip-mask>]
```

*	Clears the entire ip routing table
ip-addr	IP address
ip-mask	IP mask address

Example:

```
Router-N# clear ip route 192.168.49.1 255.255.255.0
```


configure

User level: privileged, supervisor.

Use the `configure` command to enter configure mode.

The syntax for this command is:

```
configure
```

Example:

```
P330-1(super)# configure
Router-N(configure)#
```

copy module-config scp

Use the `copy module-config scp` command to upload the switch-level parameters from the current NVRAM running configuration into a file via SCP.

The syntax for this command is:

```
copy module-config scp <filename> <ip> <mod_num>
```

<code>filename</code>	The file name (full path)
<code>ip</code>	The IP address of the SCP server
<code>mod-num</code>	The switch number

Example:

```
P330-N# copy module-config scp c:\config\switch1.cfg 192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****
```


copy module-config tftp

Use the `copy module-config tftp` command to upload the switch-level parameters from the current NVRAM running configuration into a file via TFTP.

The syntax for this command is:

```
copy module-config tftp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the TFTP server
mod-num	The switch number

Example:

```
P330-N# copy module-config tftp c:\config\switch1.cfg 192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show tftp upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations.                                     *
*****
```

copy running-config scp

Use the `copy running-config scp` command to upload the current switch-level parameters from the current NVRAM running configuration into a file via SCP.

The syntax for this command is:

```
copy running-config scp <filename> <ip> <mod_num>
```

filename	The file name (full path)
ip	The IP address of the SCP server
mod-num	The switch number

Example:

```
P330-N# copy running-config scp c:\config\switch1.cfg 192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****
```

copy running-config startup-config

User level: privileged, supervisor.

Use the `copy running-config startup-config` command to save the policy and router configurations to the startup configuration file in the NVRAM.

The syntax for this command is:

```
copy running-config startup-config
```

Example:

```
Router-N(super)# copy running-config startup-config
```

copy running-config tftp

User level: privileged, supervisor.

Use the `copy running-config tftp` command to upload the active policy and router configurations to a TFTP server.

The syntax for this command is:

```
copy running-config tftp <filename> <ip>
```

filename Destination file name in the tftp server (full path).

ip The ip address of the tftp server.

Example:

```
Router-N(super) # copy running-config tftp c:\P330-ML\startup.cfg 149.49.100.41
```

Example: (for Unix):

```
Router-N(super) # copy running-config tftp /folder/P330-ML/startup.cfg 149.49.100.41
```

copy scp module-config

User level: privileged, supervisor.

Use the `copy scp module-config` command to download a module configuration to the device via SCP.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvrाम initialize` command.

The syntax for this command is:

```
copy scp module-config <filename> <ip>
```

filename Source file name on the SCP server (full path).

ip The ip address of the SCP server.

Example (for Windows):

```
P330-N# copy scp module-config c:\P330-ML\module.cfg 149.49.100.41
```

Example: (for Unix):

```
P330-N# copy scp module-config /folder/P330-ML/module.cfg 149.49.100.41
```

copy scp startup-config

User level: privileged, supervisor.

Use the `copy scp startup-config` command to download a startup configuration to the device via SCP.

- ① Only parameters that differ from the factory default settings for the switch are included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

copy scp startup-config <filename> <ip>

filename Source file name on the SCP server (full path).

ip The ip address of the SCP server.

Example (for Windows):

```
P330-N# copy scp startup-config c:\P330-ML\startup.cfg  
149.49.100.41
```

Example: (for Unix):

```
P330-N# copy scp startup-config /folder/P330-ML/  
startup.cfg 149.49.100.41
```

copy startup-config scp

Use the `copy startup-config scp` command to upload the switch-level startup configuration from the active bank into a file via SCP.

The syntax for this command is:

`copy startup-config scp` <filename> <ip> <mod_num>

filename The file name (full path)

ip The IP address of the SCP server

mod-num The switch number

Example:

```

P330-N# copy startup-config scp c:\config\switch1.cfg 192.168.49.10 5
Beginning upload operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
For more information , use 'show upload status' command

*****
* If you are currently running the P330-ML Device Manager
application,*
* it is recommended to exit from it before performing configuration*
* download operations. *
*****

```

copy startup-config tftp

User level: privileged, supervisor.

Use the `copy startup-config tftp` command to upload the policy and router startup configurations to a TFTP server.

The syntax for this command is:

```
copy startup-config tftp <filename> <ip>
```

`filename` Destination file name in the tftp server (full path).

`ip` The ip address of the tftp server.

Example:

```

Router-N(super) # copy startup-config tftp c:\P330-
ML\startup.cfg 149.49.100.41

```

Example: (for Unix):

```

Router-N(super) # copy startup-config tftp /folder/P330-ML/
startup.cfg 149.49.100.41

```

copy tftp startup-config

User level: privileged, supervisor.

Copies the policy and router configurations from the saved TFTP file to the Startup Configuration file in the NVRAM.

① Only parameters that differ from the factory default settings for the switch are

included in the configuration file. Therefore, it is important to reinitialize the NVRAM to the factory default settings before downloading configuration files to the switch. To reinitialize the NVRAM, run the `nvr initialize` command.

The syntax for this command is:

```
copy tftp startup-config <filename> <ip>
```

filename	file name (full path)
ip	The ip address of the host

Example:

```
Router-N> copy tftp startup-config c:\P330-ML\router1.cfg  
192.168.49.10
```

disconnect ssh

User level: supervisor

Use the `disconnect ssh` command to disconnect an SSH session.

The syntax for this command is:

```
disconnect ssh <session-id>
```

session-id	The SSH session ID. Use the <code>show ssh</code> command to learn an SSH session ID.
------------	---

Example:

```
P330-ML-2# disconnect ssh 0x508622f0  
  
You are about to close this session - do you want to  
continue (Y/N)? y  
  
Closing session 0x508622f0
```

erase startup-config

Use the `erase startup-config` command to clear the startup configuration.

The syntax for this command is:

```
erase startup-config
```

Example:

```
Router-N(configure)# erase startup-config
```

event log

Use the `event log` command to display a list of the event messages.

① The event messages shown are encrypted and are reserved for Avaya use only.

The syntax for this command is:

```
event log [<num>]
```

`num` Number of event messages to display (max=30)

Example:

```
Router-N(configure)# event log
The following message is for internal use only!!!

Z,o(9?+.ig?aDZ_Z0"Dw"ZHlJZZ,300R3333aDZt?(Z
Zt?(Z?qDZ?qXZ;z=WZYLd{z5^=}ZHt!Z^YYE
Z33D@3D3YDRTDQTD3wZ'E~MZw@T:@T:_@:_QZ~NZz'oYPZw
Z,o(9?+.ig?aDZ"Z0"D3"ZHlJZZ,300R3333aDZt?(Z
Zt?(Z?qDZ?qXZ;z=WZYLd{z5^=}ZHt!Z^YYE
Z33D@3D3YDRTDQTD3wZ'E~MZw@T:@T:_@:_QZ~NZz'oYPZw
Z,=H^zNaDZ0Z3D33ZHlJZZ,303"3333aDZ?lU19ojoiz Z(""?
A\Zlit?ign
Z,!AoaDZwZ0Q_D_QZHlJZZ,303w3333aDZgjKZ ZZ}>}N=Z{~/Z5{ }^E}Y
Done!
```

exit

User level: user, privileged, supervisor

Use the `exit` command to return to the previous context or disconnect from the switch.

The syntax for this command is:

```
exit
```

Example:

```
Router-N(configure router:rip)# exit  
Router-N(configure)#
```

fragment chain

Use the **fragment chain** command to set the maximum number of fragments that can comprise a single IP packet destined to the router. Use the **no** form of this command to set the fragment chain to the default value (64).

- ① The router does not perform reassembly of packets in transit.

The syntax for this command is:

```
[no] fragment chain <chain-limit>
```

chain-limit The maximum number of fragments that can comprise a single IP packet, from 2 to 2048. The default is 64.

Example:

```
Router-N# fragment chain 30
```

fragment size

Use the **fragment size** command to set the maximum number of fragmented IP packets, destined to the router, to reassemble at any given time. Use the **no** form of this command to set the fragment size to the default value (100).

- ① The router does not perform reassembly of packets in transit.

The syntax for this command is:

```
[no] fragment size <database-limit>
```

database-limit The maximum number of packets undergoing re-assembly at any given time, from 0 to 200. The default is 100.

Example:

```
Router-N# fragment size 150
```

fragment timeout

Use the **fragment timeout** command to set the maximum number of seconds to reassemble a fragmented IP packet destined to the router. Use the **no** form of this command to set the fragment timeout to the default value (10).

① The router does not perform reassembly of packets in transit.

The syntax for this command is:

```
[no] fragment timeout <timeout>
```

timeout	The maximum number of seconds to re-assemble an IP packet, from 5 to 120. The default is 10.
---------	--

Example:

```
Router-N# fragment timeout 30
```

help

User level: user, privileged, supervisor

Use the **help** command to obtain help on CLI commands.

The syntax for this command is:

```
help <command>
```

command	A specific CLI command or group of commands
---------	---

Example:

```
Router-N> help arp
Arp commands:
-----
Syntax : [no] arp <ip addr> <mac addr>
        <ip addr>      - IP address
        <mac addr>     - MAC address
Examples:  arp 137.22.33.44 00:11:22:33:44:55
          no arp 137.22.33.55

arp timeout                Set the ARP timeout
```

hostname

User level: privileged, supervisor.

Use the `hostname` command to change the system prompt used for the router

Use the `no hostname` command to return the system prompt to its default.

This command does not change the system prompt of the switch. To change the system prompt of the switch, use the host name command in the Layer 2 tree.

The syntax for this command is:

```
[no] hostname [<hostname_string>]
```

<code>hostname_string</code>	The string to be used as the hostname (up to 20 characters). If you do not enter a string, the current hostname is displayed.
------------------------------	--

Example:

```
Router-N> hostname Marketing
Marketing-1 #
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

icmp in-echo-limit

User level: privileged, supervisor.

Use the `icmp in-echo-limit` command to set the number of echo requests per second that the router will reply.

Use the `no icmp in-echo-limit` command to restores the value to its default.

The syntax for this command is:

```
icmp in-echo-limit <size>
```

size The rate of echo requests per second. Value range = 1 to 1000. Default = 50.

Example:

```
Router-N# icmp in-echo-limit 100
Done!
```

interface

User level: privileged, supervisor.

Use the `interface` command to create and enter the Interface Configuration Mode.

Use the `no interface` command to delete a specific IP interface.

The syntax for this command is:

```
[no] interface <interface name>
```

interface name String (up to 32 characters). This name should not start with the letters "def".

Example:

```
Router-N(configure) # interface marketing
Done!
Router-1(config-if:marketing) #
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

ip access-default-action

User level: privileged, supervisor.

Use the `ip access-default-action` command to set the default action for a specific policy list.

The syntax for this command is:

```
ip access-default-action <policy-list-number> <default-
```

action>

<policy-list-number> integer (100 - 149)
<default-action> permit | deny

Example:

```
Router-N(configure)# ip access-default-action 101 default-  
action-deny  
Done!
```

ip access-group

User level: privileged, supervisor.

Use the `ip access group` command to activate a specific policy list.

The syntax for this command is:

ip access-group <policy-list-number> <default-action>

<policy-list-number> integer (100 - 149)
<default-action> permit | deny

Example:

```
Router-N(configure)# ip access-group 101  
Done!
```

ip access-list

User level: privileged, supervisor.

Use the `ip access list` command to create a specific policy rule. The access list contains several of these rules: each rule pertains to the source IP address, the destination IP address, the protocol, the protocol ports (if relevant), and to the ACK bit (if relevant).

Use the `no ip access list` command to delete a specific rule.

The syntax for this command is:

```
[no] ip access-list <access-list-number> <access-list-index>  
                                         <command> <protocol> {<source-ip>  
                                         <source-wildcard> | any | host
```

```
<source-ip> [<operator> <port> [<port>]]
{<destination-ip> <destination-
wildcard> | any | host
<destination-ip> [<operator> <port>
 [<port>]] [established] [precedence]
```

access-list-number	integer (100 - 149)
access-list-index	integer (1 - 9999)
command	permit deny deny-and-notify fwd0-7
protocol	ip tcp udp integer (1 - 255)
source-ip	ip network
source-wildcard	ip network wildcard
operator	eq lt gt range
port	integer (1 - 65535)
destination-ip	ip network
destination-wildcard	ip network wildcard
precedence	mandatory optional

Example:

```
Router-N# ip access-list 101 23 deny ip any
1.2.0.0 0.0.255.255
```

ip access-list-cookie

User level: privileged, supervisor.

Use the `ip access-list-cookie` command to set the list cookie for a specific policy list.

The syntax for this command is:

```
ip access-list-cookie <policy-list-number> <cookie>
```

policy-list-number	integer (100 - 149). 0 is the default list
cookie	integer

action <action> = permit | deny | deny-and-notify | fwd0 | fwd1 - fwd7

- permit: do nothing, let the packet pass:
- deny: drop the packet
- deny-and-notify: drop the packet and send an SNMP trap
- fwd0, fwd1fwd7: Set the frame COS field to 0,7

Example:

```
Router-N(configure) # ip access-list-dscp operation 101 0-63
permit
Router-N(configure) # ip access-list-dscp operation 101 62
fwd5
```

ip access-list-dscp trust

User level: privileged, supervisor.

Use the `ip access-list-dscp trust` command to decide which original frame fields influence the selection of packet priority.

① This command does not apply to the P333R.

The syntax for this command is:

```
ip access-list-dscp trust <policy-list-number>
{untrusted|trust-cos |trust-dscp}
```

policy-list-number A valid id number for a policy list currently defined for the module (100 - 149)

untrusted Forward the packet with priority 0

trust-cos Forward the packet with its original 802.1p priority (default)

trust-dscp Forward the packet with the maximum priority between 802.1p and the priority obtained from the DSCP-CoS mapping table

Example:

```
Router-N(configure) # ip access-list-dscp trust 100 trust-  
dscp  
Done!
```

ip access-list-name

User level: privileged, supervisor.

Use the `ip access-list-name` command to set a name for a policy list.

The syntax for this command is:

```
ip access-list-name <policy-list-number> <name>
```

<policy-list-number> integer (100 - 149)

<name> list name

Example:

```
Router-N(configure) # ip access-list-name 101 morning
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

ip access-list-owner

User level: privileged, supervisor.

Use the `ip access-list owner` command to set the owner for a specific policy list.

The syntax for this command is:

```
ip access-list-owner <policy-list-number> <owner>
```

<policy-list-number> integer (100 - 149)

<owner> list owner

Example:

```
Router-N(configure) # ip access-list-owner 101 admin  
Done!
```

ip bootp-dhcp relay

User level: privileged, supervisor.

① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode if necessary.

The `ip bootp-dhcp` command enables relaying of bootp and dhcp requests to the bootp/dhcp server.

The `no ip bootp-dhcp` command disables bootp/dhcp relay.

The default state is disabled.

The syntax for this command is:

```
[no] ip bootp-dhcp relay
```

Example:

To enable relaying of BOOTP and DHCP requests:

```
Router-N(configure) # ip bootp-dhcp relay  
Done!
```

To disable relaying of bootp and dhcp requests:

```
Router-N(configure) # no ip bootp-dhcp relay  
Done!
```

ip default-gateway

User level: privileged, supervisor.

- ① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `ip default-gateway` command to define a default gateway (router).

Use the `no ip default gateway` command to remove the default gateway.

The syntax for this command is:

```
[no] ip default-gateway <ip-address> [<cost>] [<preference>]
```

ip-address	The IP address of the router.
cost	The path cost. The default is 1
preference	Preference, either High or Low. Default is Low.

Example:

To define the router at address 192.168.37.1 as the default gateway:

```
Router-N(configure)# ip default-gateway 192.168.37.1
```

ip max-arp-entries

User level: privileged, supervisor.

- If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `ip max-arp-entries` command to set the maximum number of ARP cache entries allowed in the ARP cache.

Use the `no ip max-arp-entries` command to restore the default value of 4096.

- ① For this command to take effect, run the `copy running-config startup-config` command and reset the device.

The syntax for this command is:

```
[no] ip max-arp-entries <value>
```

value	The space available for the IP address table. When you decrease the number of entries, it may cause the table to be relearned more frequently. If you do not enter a value, then the current ARP Cache size is shown.
-------	---

Example:

To set the maximum number of ARP cache entries to 8000:

```
Router-N(configure) # ip max-arp-entries 8000
```

To restore the maximum number of ARP cache entries to its default:

```
Router-N(configure) # no ip max-arp-entries
```

ip max-route-entries

User level: privileged, supervisor.

① If you are at the "privileged" level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

The `ip max-route-entries` command exists for compatibility with Avaya™ P550. There is no limitation on the size of the routing table, except for the amount of available memory.

Use the `no ip max-route-entries` command to remove the limitation.

① For this command to take effect, run the `copy running-config startup-config` command and reset the device.

The syntax for this command is:

```
[no] ip max-route-entries <value>
```

value	Number of entries
-------	-------------------

Example:

```
Router-N(configure) # ip max-route-entries 4000
```

ip netmask-format

User level: privileged, supervisor.

① If you are at the "privileged" level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode.

Use the `ip netmask-format` command to specify the format of netmasks in the `show` command output.

Use the `no ip netmask-format` command to restores the default format which is

a dotted decimal.

The syntax for this command is:

```
[no] ip netmask-format <mask-format>
```

The possible mask formats are:

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example 17
decimal	The network masks are in dotted decimal notation. For example, 255.255.255.0.
hexadecimal	The network masks are in hexadecimal format as indicated by the leading 0X. For example, 0FFFFFFF00.

Example:

To display netmasks in decimal format:

```
Router-N(configure)# ip netmask-format bitcount decimal  
Done!
```

ip ospf router-id

User level: privileged, supervisor.

Use the `ip ospf router-id` command to configure the router identity.

Use the `no ip ospf router-id` command to return the router identity to its default (the lowest existing IP interface).

The syntax for this command is:

```
[no] ip ospf router-id <router id>
```

router-id	The IP address of the router.
-----------	-------------------------------

Example:

```
Router-N(configure router:ospf) # ip ospf router-id
192.168.49.1
```

ip route

User level: privileged, supervisor.

- ① If you are at the "privileged" level, you can only access this command in Configure mode. Type **configure** at the command prompt to enter configure mode.

Use the `ip route` command to establish a static route.

Use the `no ip route` command to remove a static route.

You can edit (add or remove), individually, each one of the 3 possible next-hop addresses for a static route.

The syntax for this command is:

```
[no] ip route <ip-address> <mask> <next-hop> [<next-hop>]
[<next-hop>] [<cost>] [<preference>]
```

ip-address	The IP address of the network
mask	Mask of the static route
next-hop	The next hop address in the network
cost	The path cost. The default is 1
preference	Preference, either High or Low. Default is Low.

Example:

To define the router 192.168.33.38 as the next hop for the network 192.168.33.0 with mask 255.255.255.0:

```
Router-N(configure) # ip route 192.168.33.0 255.255.255.0
10.10.10.10
```

ip routing

User level: privileged, supervisor.

- ① If you are at the "privileged" level, you can only access this command in Configure mode.
Type **configure** at the command prompt to enter configure mode.

Use the `ip routing` command to enable IP routing.

Use the `no ip routing` command to disable the IP routing process in the device. By default, IP routing is enabled.

The syntax for this command is:

```
[no] ip routing
```

Example:

```
Router-N(configure)# ip routing
Router-N(configure)#
```

ip simulate

User level: privileged, supervisor.

① If you are at the "privileged" level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter Configure mode if necessary.

Use the `ip simulate` command to check the policy for a simulated packet. The command contains the addressed list number, and the packet parameters.

The syntax for this command is:

```
ip simulate <access-list-number> [<priority>] [<dscp-value>]<source> <destination> [<protocol> [<source port> <destination port> [<established>]]]
```

access-list-number	integer (100 - 149, 0 is the default list)
priority	fwd0 fwd1 - fwd7
dscp value	dscp0 dscp1 - dscp63
source	source ip address
destination	destination ip address
protocol	ip tcp udp integer (1 - 255)
source port	integer (1 - 65535)
destination port	integer (1 - 65535)
established	value of TCP established bit

Example:

```
Router-N(configure)# ip simulate 100 192.67.85.12
193.76.54.25
```

ping

User level: user, privileged, supervisor

Use the ping command to send ICMP echo request packets to another node on the network.

- ① You can use this command via the master switch only.
- ① The command is executed until you

The syntax for this command is:

```
ping <host> [<interval> [<size> [<timeout> [<source
address>]]]]]
```

host	Host IP address/Internet address of route destination. If missing then the last host IP is used.
interval	Interval between ping commands in seconds (1 to 256)
size	Size of packet in bytes (22 to 66500)
timeout	Timeout in seconds (1 to 10)
source address	IP address of one of the router interfaces

Example: to ping the IP number 149.49.48.1 three times:

```
Router-N> ping 149.49.48.1 3

PING 149.49.48.1: 56 data bytes
64 bytes from 149.49.48.1: icmp_seq=0. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=1. time=0. ms
64 bytes from 149.49.48.1: icmp_seq=2. time=0. ms

----149.49.48.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

prompt-length

User level: privileged, supervisor.

Use the CLI `prompt length` command to set the length of the command prompt that is displayed.

The syntax for this command is:

```
prompt-length <full | prompt-size>
```

full	return the CLI prompt to its full length
------	--

prompt-size	size of the CLI prompt in characters
-------------	--------------------------------------

Example:

```
Router-N> prompt-length 3  
~N>
```

reset

User level: user, privileged, supervisor

Use the `reset` command to restart an individual switch.

The syntax for this command is:

```
reset
```

Example:

```
Router-N> reset  
This command will force a switch-over to the master module  
and disconnect your telnet session.  
Do you want to continue (y/n) [n]? y  
Connection closed by foreign host.
```

router ospf

User level: privileged, supervisor.

- ① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter interface mode.

Use the `router ospf` command to enable the OSPF protocol on the system and enter the “router ospf” context.

Use the `no router ospf` command to disable the OSPF one the system.

The default is **disabled**.

The syntax for this command is:

```
[no] router ospf
```

Example:

```
Router-N(configure) # router ospf
Done!
Router-N(configure router:ospf) #
```

router rip

User level: privileged, supervisor.

① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter interface mode.

Use the `router rip` command to configure the Routing Information Protocol (RIP) and enter the “router rip” context.

Use the `no router rip` command to disable RIP.

The default state is disabled.

The syntax for this command is:

```
[no] router rip
```

Example:

To enable the RIP protocol:

```
Router-N(configure) # router rip
Done!
Router-N(configure router:rip) #
```

router srrp

User level: privileged, supervisor.

① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode if necessary.

Use the `router srrp` command to enable srrp redundancy for the main router and enter the “router srrp” context.

Use the `no router srrp` command to disable srrp redundancy for the main router.

Example:

To enable the srrp:

```
Router-N(configure)# router srrp
Done!
Router-N(configure router:srrp)#
```

router vrrp

User level: privileged, supervisor.

① If you are at the “privileged” level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter configure mode if necessary.

Use the `router vrrp` command to enable VRRP router redundancy globally.

Use the `no router vrrp` command to disable VRRP router redundancy.

The syntax for this command is:

```
[no] router vrrp
```

Example:

```
Router-N(configure)# router vrrp
Done!
```

session

User level: user, privileged, supervisor

Use the `session` command to open a session with a specific entity in a switch of the stack. For example, you can open a session with the Routing entity of a P332G-ML switch in the stack.

The syntax for this command is:

```
session [<mod_num> [switch|router|atm|mgp|wan]]
```

`mod_num`

(optional) The switch number.

If you do not specify this parameter, you will get the default entity of the stack (Layer 2 session to the Master)

switch | router | atm | mgp | wan (optional) The entity to which you want to open a session.
 If you do not specify this parameter, you will get the default entity of the specific module:
 switch - Layer 2 entity of the switch (see Note below).
 router - Routing entity.
 atm - ATM entity.
 mgp - Media Gateway Processor.
 wan - WAN access router entity.

① When you use the `session` command the security level stays the same.

Example:

```
Router-1> session 2
Router-2>
```

① The security level stays the same when you use the `session` command.

set device-mode

User level: privileged, supervisor.

Use the `set device-mode` command to change the basic mode of operation of the switch between Router and Layer 2 modes.

① This command is available on P330-ML-ML and P333R switches only.

The syntax for this command is:

```
set device-mode <mode>
```

mode Router | Layer2

Example:

```
Router-N> set device-mode Layer2
This command will RESET the device
*** Reset *** - do you want to continue (Y/N)? y
```

set policy type

User level: privileged, supervisor.

- ① This command is available on the P334T-ML switch in device mode “Router” only.

Use the `set policy type` command to set whether the P334T-ML module enforces the active policy-list on all packets or only on routed packets (for modules in 'device-mode router').

The syntax for this command is:

```
set policy type <value> all | router
```

value	all - apply policy to all packets entering the P334T-ML through Fast Ethernet ports
	router - apply policy on routed packets only

Example:

```
Router-N# set policy type all
```

set qos policy-source

User level: privileged, supervisor.

- ① If you are at the “privileged” level, you can only access this command in Configure mode.
Type **configure** at the command prompt to enter Configure mode if necessary.

Use the `set qos policy-source` command to set the policy source (local or policy server).

The syntax for this command is:

```
set policy source <source>
```

source	local or policy server
	<ul style="list-style-type: none">• The default policy source for P330-ML-ML switches is <i>local</i>• The default policy source for P333R and P333R-LB switches is <i>policy-server</i>

Example:

```
Router-N# set qos policy-source local
Done!
```

set system contact

User level: user, privileged, supervisor

Use the `set system contact` command to set the system contact MIB variable.

The syntax for this command is:

```
set system contact [string]
```

string System contact

Example:

```
Router-N(super) # set system contact "gregory kohll"
Done!
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

set system location

User level: user, privileged, supervisor

Use the `set system location` command to set the system location MIB variable

The syntax for this command is:

```
set system location [string]
```

string System name

Example:

```
Router-N(super) # set system location "tech support"
Done!
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

set system name

User level: privileged, supervisor.

Use the `set system name` command to set the mib2 system name MIB variable.

The syntax for this command is:

```
set system name [string]
```

- | | |
|--------|---|
| string | <ul style="list-style-type: none">• The system name string should be typed inside inverted commas.• The name is cleared if you leave this field blank. |
|--------|---|

Example:

```
Router-N(super)# set system name P330-ML-1  
Done!
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

set vlan

User level: privileged, supervisor.

- ① If you are at the "privileged" level, you can only access this command in Configure mode.

Type **configure** at the command prompt to enter Configure mode if necessary.

Use the `set vlan` command to create a router Layer 2 interface.

The syntax for this command is:

```
set vlan <vlan-id> name <vlan-name>
```

vlan-id	VLAN number
vlan-name	VLAN name

Example:

```
Router-N(configure)# set vlan 2 name vlan2
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

show copy status

User level: user, privileged, supervisor

Use the `show copy status` command to show the status of the local configuration copy operation.

The syntax for this command is:

```
show copy status
```

Example:

```
Router-N> show copy status
Module #1
=====
Module           : 1
Source file      : .router-startup
Destination file : .router-running
Host             : -
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

show device-mode

User level: user, privileged, supervisor

- ① This command does not apply to the P333R-LB which is always in “Load Balancing” mode.

Use the `show device-mode` command to show the current switch operating mode. Possible modes are Router or Switch.

The syntax for this command is:

```
show device-mode
```

Example:

```
Router-N> show device mode  
Device mode is router
```

show download status

User level: user, privileged, supervisor

- ① This command applies the P330-ML-ML switches only.

Use the `show download status` command to display a summary of the last software download operation.

The syntax for this command is:

```
show download status [slot]
```

Example:

```
P330-N>show download status 1  
Module #1  
=====  
Module           : 1  
Source file       : c:\session4.txt  
Destination file  : module-config  
Host              : 149.49.75.100  
Running state     : Idle  
Failure display   : SCP - Server refused  
Last warning      : No-warning  
Bytes Downloaded : 0
```

show erase status

User level: user, privileged, supervisor

Use the `show erase status` command to view the status of the erase

configuration operation.

The syntax for this command is:

```
show erase status
```

show fragment

User level: user, privileged, supervisor

Use the `show fragment` command to display information regarding fragmented IP packets that are destined to the router.

① The router does not perform reassembly of packets in transit.

This command displays the following information:

Size	Maximum number of packets set by the <code>fragment size</code> command
Chain	Maximum number of fragments for a single packet set by the <code>fragment chain</code> command.
Timeout	Maximum number of seconds set by the <code>fragment timeout</code> command.
Queue	Number of packets currently awaiting reassembly.
Assemble	Number of packets successfully reassembled
Fail	Number of packets which failed to be reassembled
Overflow	Number of packets which overflowed the fragment database.

The syntax for this command is:

```
show fragment
```

Example:

```
Router-N> show fragment
Max number of concurrently reassembled packets is 100
Max number of fragments per packet is 64
Fragment timeout is 10 sec
Number of packets waiting to be reassembled is 0
Number of successfully reassembled packets is 11954
Number of packets which failed to be reassembled is 0
Number of packets which overflowed the database is 0
```

show ip access-group

User level: user, privileged, supervisor

Use the `show ip access-group` command to see information about the configured active access list.

① This command is available on P330-ML-ML switches only.

The syntax for this command is:

```
show ip access-group
```

Example:

```
Router-N> show ip access-group  
access-group 100
```

show ip access-lists

User level: user, privileged, supervisor

Use the `show ip access lists` command to display all the current policy lists.

The syntax for this command is:

```
show ip access-lists [<policy-list-number>]
```

<code>policy-list-number</code>	The policy list number (integer from 100 to 149; 0 is the default list).
---------------------------------	--

Example:

```
Router-N> show ip access-lists  
The current policy source is local  
default List (0) parameters  
List Owner : other  
List 0 is valid  
default action for list 0 is permit
```

show ip access-list-dscp

User level: user, privileged, supervisor

Use the `show ip access-list-dscp` command to display the DSCP to CoS map of a policy-list.

The syntax for this command is:

```
show ip access-list-dscp <policy-list-number> [<dscp>]
```

policy-list-number	A valid id number for a policy list currently defined for the module (100 - 149, 0 - default list)
dscp	dscp entry (0 - 63)

Example:

```
Router-N> show ip access-list-dscp 101
Trust configuration is trust-cos
DSCP      Action          Precedence      Name
-----
0         fwd0             mandatory      DSCP#0
1         fwd0             mandatory      DSCP#1
2         fwd0             mandatory      DSCP#2
3         fwd0             mandatory      DSCP#3
4         fwd0             mandatory      DSCP#4
5         fwd0             mandatory      DSCP#5
6         fwd0             mandatory      DSCP#6
7         fwd0             mandatory      DSCP#7
8         fwd1             mandatory      DSCP#8
9         fwd1             mandatory      DSCP#9
10        fwd1             mandatory      DSCP#10
11        fwd1             mandatory      DSCP#11
```

show ip access-list-summary

User level: user, privileged, supervisor

① This command applies to the P334T-ML only.

Use the `show ip access-list-summary` command to display a list of all configured access lists.

The syntax for this command is:

```
show ip access-list-summary
```

Example:

```
Router-N> show ip access-list-summary
The policy lists summary:
default List (0)
```

show ip arp

User level: user, privileged, supervisor

Use the `show ip arp` command to display the Address Resolution Protocol (ARP) cache.

The syntax for this command is:

```
show ip arp [<if-name> | <vlan> | <ip addr> | <ip-mask> static]
```

<code>if-name</code>	Interface name (string up to 32 chars)
<code>vlan</code>	VLAN NAME (string up to 16 chars) or VLAN ID (number)
<code>ip-addr</code>	The IP address of the station(s)
<code>ip-mask</code>	The ip mask of the routes.
<code>static</code>	Display static ip ARP information.

Example:

```
Router-N> show ip arp
Showing 3 rows
  Address          MAC Address      Interface  Type      TTL
-----
192.168.54.1      00:40:0d:8c:12:01  mgmt      Dynamic   14360
192.168.2.33      00:40:0d:5c:14:01  loco      Static    Not Aged
192.168.1.111     00:40:0d:5d:72:01  ppp       Static    Not Aged
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

show ip icmp

User level: user, privileged, supervisor

Use the `show ip icmp ip` command to display the status of ICMP error messages.

The syntax for this command is:

```
show ip icmp
```

Example:

```
Router-N> show ip icmp  
  
ICMP error messages status is ENABLE
```

show ip interface

User level: user, privileged, supervisor

Use the `show ip interface` command to display information for an IP interface.

The syntax for this command is:

```
show ip interface [<interface>] |<vlan> |<IP addr>]
```

interface	The name of the interface whose information you want to display.
vlan	The name or ID of the VLAN over which there are interfaces you want to display.
ip-address	The IP address of the interface whose information you want to display.

Example:

```
Router-N> show ip interface
Showing 2 Interfaces
mgmt is administratively up
  On vlan Default
  Internet address is 10.49.54.14    , subnet mask is
255.255.255.0
  Broadcast address is 10.49.54.255
  Directed broadcast forwarding is disabled
  Proxy ARP is disabled

baba is administratively down
  On vlan v2
  Internet address is 192.168.0.14    , subnet mask is
255.255.0.0
  Broadcast address is 192.168.255.255
  Directed broadcast forwarding is disabled
  Proxy ARP is disabled
```

- ❶ If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example "new york".

show ip interface brief

User level: user, privileged, supervisor

Use the `show ip interface brief` command to display brief information for an IP interface.

The syntax for this command is:

```
show ip interface [<interface>|<vlan>|<ip-address>]
```

interface	The name of the interface whose information you want to display - a string of up to 32 characters.
ip-address	The IP address of the interface whose information you want to display.
vlan	The name or ID of the VLAN over which there are interfaces you want to display - a string of up to 32 characters.

Example:

```
Router-N> show ip interface brief
Showing 1 Interfaces
-----
Interface                Address            Mask                Status
-----
net                       149.49.54.56     255.255.255.0     up
```

show ip ospf

User level: user, privileged, supervisor

Use the `show ip ospf` command to displays general information about OSPF routing.

The syntax for this command is:

```
show ip ospf
```

Example:

```
Router-N> show ip ospf
Routing Process OSPF with ID 149.49.75.222
Number of areas in this router is 1
Area 0.0.0.0
Number of Interfaces in this area 0
SPF algorithm executed 1 times
SPF hold time is 3 sec
```

show ip ospf database

User level: user, privileged, supervisor

Displays lists of information related to the OSPF database for a specific router.

The syntax for this command is:

```
show ip ospf database [<ls type>]
```

ls-types:

asbr-summary	Displays information only about the autonomous system boundary router summary LSAs. Optional.
router	Displays information only about the router LSAs. Optional.

network	Displays information only about the network LSAA. Optional.
network-summary	Displays information only about the network LSAA summary. Optional
external	Displays information only about the external LSAA. Optional.

show ip ospf interface

User level: user, privileged, supervisor

Use the `show ip ospf interface` command to display OSPF-related interface information.

The syntax for this command is:

```
show ip ospf interface [<interface-name>]
```

interface-name The OSPF interface name.

Example:

```
Router-N> show ip ospf interface  
There are no OSPF interfaces
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

show ip ospf neighbor

User level: user, privileged, supervisor

Displays OSPF-neighbor information on a per-interface basis.

The syntax for this command is: **show ip ospf neighbor**
[<interface-name>] [<neighbor-id>]

interface-name The OSPF interface name.

neighbor-id Neighbor ID.

show ip reverse-arp

User level: user, privileged, supervisor

Use the `show ip reverse-arp` command to display the IP address of a host, based on a known MAC address.

The syntax for this command is:

```
show ip reverse-arp <mac addr> [<match len>]
```

`mac addr` MAC address

`match len` The number of bytes in the address to match

Example:

```
Router-N> sh ip reverse-arp 00:10:a4:98:97:e0
```

Showing 1 rows

Address	MAC Address	I/F	Type	TTL
149.49.70.68	00:10:a4:98:97:e0	e-70	Dynamic	14355

show ip route

User level: user, privileged, supervisor

Use the `show ip route` command to display information about the IP unicast routing table.

The syntax for this command is:

```
show ip route
```

```
Router-N> show ip route
```

Showing 2 rows

Network	Mask	Interface	Next-Hop	Cost	TTL	Source
0.0.0.0	0.0.0.0	net	149.49.54.1	1	n/a	STAT-LO
149.49.54.0	255.255.255.0	net	149.49.54.56	1	n/a	LOCAL

show ip route best-match

User level: user, privileged, supervisor

Use the `show ip route best-match` command to display a routing table for a destination address.

The syntax for this command is:

```
show ip route best-match <dst addr>
```

dst addr IP address

Example:

```
Router-N> show ip route best-match 199.93.0.0
Searching for: 199.93.0.0
Showing 1 rows
Network          Mask             Interface        Next-Hop         Cost TTL   Source
-----
199.93.0.0      255.255.0.0     e-135new        135.64.76.1     1   n/a   STAT-HI
```

show ip route static

User level: privileged, supervisor.

Use the `show ip static route` command to display the static routes.

The syntax for this command is:

```
show ip route static [<ip addr> [<mask>] ]
```

ip-address The IP address of the routes

mask The ip mask of the routes.

Example:

```
Router-N> sh ip route static
Showing 34 rows
Network          Mask             Interface        Next-Hop         Cost Pref Active
-----
10.0.8.0         255.255.255.0   e-36             149.49.36.11    1   high Yes
135.0.0.0        255.0.0.0       e-135new         135.64.76.1     1   high Yes
135.64.0.0       255.255.0.0     e-135            135.87.164.1    1   high No
149.49.0.0       255.255.0.0     trial            10.10.254.253   1   low  Yes
149.49.2.0       255.255.255.0   n/a              v-Route-FW 1     1   high Yes
```

show ip route summary

User level: user, privileged, supervisor

Use the `show ip route summary` command to display the number of routes known to the switch.

The syntax for this command is:

```
show ip route summary
```

Example:

```
Router-N> sh ip route summary
```

Route Source	Networks	Subnets
Local	0	1
Static	0	1
Total	0	2

show ip ssh

User level: supervisor

Use the `show ip ssh` command to display active SSH connections.

The syntax for this command is:

```
show ip ssh
```

Example:

```
P330-N>show ip ssh
```

```
Ssh Engine: Enable  
Max Sessions: 2  
Key Type: DSA , 768 bit  
Listen Port: 22  
Ciphers List: 3des-cbc
```

Session-Id	Version	Encryption	User	IP:Port
0x508622f0	2	3des-cbc	root	135.64.100.73:4201

show ip srrp

User level: user, privileged, supervisor

Use the `show ip srrp` command to display SRRP statistics.

The syntax for this command is:

```
show ip srrp
```

Example:

```
Router-N> sh ip srrp
Admin status   Oper State   Poll interval   Timeout
-----
ENABLE         INACTIVE     1               12

Showing 1 rows

Intf IP addr      Main router addr Status
-----
149.49.54.58    0.0.0.0
```

show ip traffic

User level: user, privileged, supervisor

❶ This command does not apply to the P333R-LB.

Use the `show ip traffic` command to display the IP traffic statistics counters.

The syntax for this command is:

```
show ip traffic
```

Example:

```
Router-N> show ip traffic
IP statistics:

    Received:
    1365359 total, 45659 local destination
    0 bad hop count, 0 packet header errors
    0 unknown protocol, 136786 address errors
    1182914 discarded

    Fragments:
    0 reassembled, 0 timeouts
    0 couldn't reassemble, 0 fragmented

    Sent:
    19442 generated, 0 forwarded
    0 no route, 0 discarded
ICMP statistics:
    Received:
    881 total, 3 ICMP errors
    0 unreachable, 0 time exceeded
    0 parameter, 0 quench
    861 echo, 17 echo reply
    0 timestamps request, 0 timestamp reply
--type q to quit or space key to continue--
    0 mask requests, 0 mask replies

    0 redirects

    Sent:
    1311 total, 0 ICMP errors
    433 unreachable, 0 time exceeded
    0 parameter, 0 quench
    17 echo, 861 echo reply
    0 timestamps request, 0 timestamp reply
    0 mask requests, 0 mask replies
    0 redirects
```

```

OSPF statistics:
  Received:
  25783 total, 0 checksum errors
  0 hello, 0 database desc
  0 link state req, 0 link state updates
  0 link state acks

  Sent:
  0 total

ARP statistics:
--type q to quit or space key to continue--
  Received:
  2191321 requests, 778439 replies

  Sent:
  443 requests, 340 replies (0 proxy)

DHCP statistics:
  Requests: 0 , Replies: 0

BOOTP statistics:
  Requests: 0 , Replies: 0

```

show ip unicast cache

User level: privileged, supervisor.

Use the `show ip unicast cache` command to list the entries in the hardware unicast cache database.

The syntax for this command is:

```
show ip unicast cache [[<src addr> <src mask>] <dst addr> <dst mask>]
```

<code>src addr</code>	The source IP address.
<code>src mask</code>	The source mask IP address.
<code>dst addr</code>	The destination IP address.
<code>dst mask</code>	The destination mask IP address.

Example:

```
Router-N> show ip unicast cache
Showing 6 Sessions.
Source IP      Destination IP  Next Hop IP    NH MAC          Vlan
=====
192.168.1.1    29.2.1.1      28.2.0.2      00.00.28.02.00.02  5
192.168.2.1    29.2.2.1      28.2.0.2      00.00.28.02.00.02  5
192.168.2.2    29.2.2.2      28.2.0.2      00.00.28.02.00.02  5
192.168.2.3    29.2.2.3      28.2.0.2      00.00.28.02.00.02  5
192.168.2.4    29.2.2.4      28.2.0.2      00.00.28.02.00.02  5
192.168.2.5    29.2.2.5      28.2.0.2      00.00.28.02.00.02  5
```

show ip unicast cache networks

User level: user, privileged, supervisor

Use the `show ip unicast cache networks` command to display a summary of networks handled by the hardware unicast cache database.

The syntax for this command is:

```
show ip unicast cache networks [<net addr> <net mask>]
```

net addr	The IP address of the network.
net mask	The mask IP address.

Example:

```
Router-N> show ip unicast cache networks
Showing 7 rows (5 networks)

Network          Mask Next Hop(s)      Total Hosts
=====
10.0.0.0         16 10.2.0.2             996
71.0.0.0         16 0.0.0.0                1
130.0.0.0        8 192.168.0.130         1124
190.0.0.0        24 10.2.0.2               250
                  192.168.0.130
191.0.0.0        24 10.2.0.2               250
                  192.168.0.130
-----
Total: 2621
```

show ip unicast cache networks detailed

User level: user, privileged, supervisor

Use the `show ip unicast cache networks detailed` command to list the networks and hosts that are handled by the hardware unicast cache database.

The syntax for this command is:

```
show ip unicast cache networks detailed[<net addr> <net mask>]
```

net addr The IP address of the network.

net mask The mask IP address.

Example:

```
Router-N> show ip unicast cache networks detailed  
192.168.6.0 24  
Showing 3 rows  
NetworkMask      IP Address  
=====          =====  
192.168.6.0      24 192.168.6.40  
                  192.168.6.53  
                  192.168.6.64
```

show ip unicast cache nextHop

User level: privileged, supervisor.

Use the `show ip unicast cache nextHop` command to list the routers that are used as next-hop routers.

The syntax for this command is:

```
show ip unicast cache nextHop
```

Example:

```
Router-N> show ip unicast cache nextHop  
Showing 2 rows  
Next Hop  
=====  
192.168.4.1  
192.168.5.1
```

show ip unicast cache summary

User level: user, privileged, supervisor

Use the `show` command to display the number of host networks and next-hops in the module's unicast cache.

The syntax for this command is:

```
show ip unicast cache summary
```

Example:

```
Router-N> show ip unicast cache summary
Cache Summary
=====
Sessions   : 11056
Hosts      : 2621
Networks   : 5
Next-Hops  : 4
```

show ip vrrp

User level: user, privileged, supervisor

Use the `show vrrp` command to display VRRP information.

The syntax for this command is:

```
show ip vrrp [<vlan> [router-id <vr-id>]][detail]
```

vlan	Filter by VLAN.
router-id	Filter by virtual router ID (1-255)
vr-id	The virtual router ID.
detail	Provide detailed information.

Example:

```
Router-N> show ip vrrp
VRRP is globally enabled
VLAN   VRID  IP Address      PriTimer  State      Since
-----
  1     1    192.168.66.23  255 1     MASTER    00:00:00
  1     2    192.168.66.24  100 1     BACKUP    00:00:00
```

show ip vrrp detail

User level: user, privileged, supervisor

Use the `show ip vrrp detail` command to display full VRRP-related information

The syntax for this command is:

```
show ip vrrp detail
```

Example:

```

Router-N> show ip vrrp detail
VRRP is globally enabled
Virtual Router on VLAN:
  Router-id:                1
  State:                    MASTER
  Priority:                  255
  Advertisement Interval:   1
  Last State Change:        00:00:00
  Override Address Ownership Rule: No
  Authentication Type:      None
  Authentication Key:       ""
  Master IP Address         192.168.66.23
  Has 1 IP addresses
  IP addresses:
    192.168.66.23
  Primary IP Address:        192.168.66.23
  Primary IP Address was chosen by default
  Preemption Mode:          enabled
  # of times Master:        2
  # of received Advertisements: 0
  # of transmitted Advertisements: 20
  # of received Advertisements with Security Violations: 0

Virtual Router on VLAN:    1
  Router-id:                2
  State:                    BACKUP
  Priority:                  100
  Advertisement Interval:   1
  Last State Change:        00:00:00
  Override Address Ownership Rule: No
  Authentication Type:      None
  Authentication Key:       ""
  Master IP Address         0.0.0.0
  Has 1 IP addresses
  IP addresses:
    192.168.66.24
  Primary IP Address:        192.168.66.23
  Primary IP Address was chosen by default
  Preemption Mode:          enabled
  # of times Master:        1
  # of received Advertisements: 0
  # of transmitted Advertisements: 13
  # of received Advertisements with Security Violations: 0

Router-N>

```

show policy type*User level: user, privileged, supervisor*

① This command is available on the P334T-ML only.

Use the `show policy type` command to show whether the module enforces the active policy-list on all packets or only on routed packets (for modules in 'device-mode router').

The syntax for this command is:

```
show policy type
```

Example:

```
Router-N# show policy type  
  
Policy type is router
```

show startup-config

User level: user, privileged, supervisor

Use the `show startup-config` command to show configuration loaded at startup.

The syntax for this command is:

```
show startup-config
```

Example:

```
Router-N> show startup-config
! Avaya Inc. P333R Switch - Router configuration
! version 4.0.5
hostname "R1-Backup"
interface "net"
ip vlan name "Default"
ip address 149.49.54.56      255.255.255.0
ip default-gateway 149.49.54.1      1 low
router ospf
```

show system

User level: user, privileged, supervisor

Use the `show system` command to display the up time, system name, location, and contact person.

The syntax for this command is:

```
show system
```

Example:

```
Router-N> show system
Uptime d,h:m:s
-----
0,2:40:55

System Name           System Location           System Contact
-----
P332_version-3.0.5   Alpha LAB                 Ygdal Naouri

Switch MAC address
-----
00 40 0d 8a 04 b4
```

show upload status

User level: user, privileged, supervisor

Use the `show upload status` commands to display the status of the current configuration file copy process from the device.

The syntax for this command is:

show upload status [`<mod_num>`]

<code>mod_num</code>	Number of the module. If you do not specify a number, upload statuses for all modules in the stack are shown.
(Optional)	

Example:

```
Router-N> show upload status 1
Module           : 1
Source file      : stack-config
Destination file : c:\conf.cfg
Host             : 149.49.36.200
Running state    : Executing
Failure display  : (null)
Last warning     : No-warning
```

show vlan

User level: user, privileged, supervisor

Use the `show vlan` command to display router Layer 3 interfaces.

The syntax for this command is:

`show vlan`

Example:

```
Router-N> show vlan
VLAN NAME          VLAN ID  VLAN MAC
-----
Default            1 02:e0:3b:1d:f9:01
```

terminal

User level: user, privileged, supervisor

Use the `terminal width` and `terminal length` commands to set the width and length of the terminal display in characters.

The syntax for this command is:

```
terminal {width|length} [<characters>]
```

Example:

```
Router-N> terminal width 80  
terminal width: 80
```

traceroute

User level: user, privileged, supervisor

Use the `traceroute` command to initiate a traceroute to a remote host.

The syntax for this command is:

```
traceroute <host>
```

host IP address.

Example:

```
Router-N> traceroute 192.168.50.13
```

validate-group

User level: privileged, supervisor.

Use the `validate-group` command to verify that all the rules in a policy list are valid.

- ❶ If there is a configuration problem with a specific rule, or with a number of rules, detailed error messages will be given.

The syntax for this command is:

```
validate-group <policy-list-number>[quiet]
```

quiet does not display error messages

Example:

```
Router-1(configure)# validate-group 101  
List 101 is valid
```


- ① The validation process may take some time to complete.

Interface Context

- ① You can only access these commands in the “interface” context.
Type **interface [name]** at the command prompt to enter the “interface” context if necessary.

default-metric

User level: privileged, supervisor.

Use the `default metric` command to set the interface RIP route metric.

Use the `no default metric` command to restore the default value.

The default metric is 1.

The syntax for this command is:

```
[no] default-metric <number>
```

number The interface RIP route metric value. The range is 1 to 15.

Example:

```
Router-N(configure-if:marketing) # default metric 10  
Done!
```

enable vlan commands

User level: privileged, supervisor.

Use the `enable vlan commands` command before configuring VLAN-oriented parameters, such as `vrrp` and `boorp-dhcp relay` that affect all interfaces on the same VLAN.

The syntax for this command is:

```
enable vlan commands
```

Example:

```
Router-N(config-if:marketing) #enable vlan commands
```

ip address

User level: privileged, supervisor.

Use the `ip address` command to assign an IP address and mask to an interface.

The syntax for this command is:

```
ip address <ip-address> <mask> [<admin-state>]
```

<code>ip address</code>	The IP address assigned to the interface.
<code>mask</code>	Mask for the associated IP subnet
<code>admin-state</code>	The administration status – either Up or Down

Example:

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the interface “marketing”:

```
Router-N(config-if:marketing) # ip address 192.168.22.33  
255.255.255.0  
Done!
```

ip admin-state

User level: privileged, supervisor.

Use the `admin-state` command to set the administrative state of an IP interface. The default state is **up**.

The syntax for this command is:

```
ip admin-state <up/down>
```

<code>up/down</code>	Administrative state of the interface. The choices are
	<ul style="list-style-type: none"> • up (active) or • down (inactive).

Example:

```
Router-N(config-if:marketing) # ip admin-state up
```

ip bootp-dhcp network

User level: privileged, supervisor.

Use the `ip bootp-dhcp network` command to configure the network from which the BOOTP/DHCP server shall allocate an address.

Use the `no ip bootp-dhcp network` command to remove a network.

- ① Multiple networks can be configured and relayed per VLAN, by repeating the `ip bootp-dhcp network` command. If more than one network is configured, then the address allocation is based on a round-robin algorithm.

The syntax for this command is:

```
[no] ip bootp-dhcp network <ip-net>
```

`ip-net` The IP address of the network.

Example:

To select the network 192.168.169.0 as the network from which an address shall be allocated for bootp/dhcp requests:

```
Router-N(configure-if:marketing) # ip bootp-dhcp network  
192.168.169.0  
Done!
```

ip bootp-dhcp server

User level: privileged, supervisor.

Use the `ip bootp-dhcp server` command to add a bootp/dhcp server to handle BOOTP/DHCP requests received by this interface.

Use the `no ip bootp-dhcp server` command to remove the server. A maximum of two servers can be added to a single interface.

The syntax for this command is:

```
ip bootp-dhcp server <ip addr>
```

`ip addr` The IP address of the server.

Example:

To add station 192.168.37.46 as a bootp/dhcp server to handle bootp/dhcp requests arriving at the interface “marketing”:

```
Router-N(configure-if:marketing) # ip bootp-dhcp server  
192.168.37.46  
Done!
```

ip broadcast-address

User level: privileged, supervisor.

Use the `ip broadcast` command to update the interface broadcast address. The Broadcast address must be filled in with 0s (zeros) or 1s (ones).

The syntax for this command is:

```
ip broadcast-address <bc addr>
```

bc addr	The broadcast IP address
---------	--------------------------

Example:

```
Router-N(config-if:marketing) #ip broadcast address  
192.168.255.255
```

ip directed-broadcast

User level: privileged, supervisor.

Use the `ip directed-broadcast` command to enable net-directed broadcast forwarding.

Use the `no ip directed-broadcast` command to disables net-directed broadcasts on an interface.

The syntax for this command is:

```
[no] ip directed-broadcast
```

Example:

```
Router-N(config-if:marketing) # ip directed broadcast
```

ip netbios-rebroadcast

User level: privileged, supervisor.

Use the `ip netbios-rebroadcast` command to set the NETBIOS rebroadcasts mode on an interface.

Use the `no ip netbios-rebroadcast` command to disable NETBIOS rebroadcasts on an interface.

The syntax for this command is:

```
[no] ip netbios-rebroadcast [<direction>]
```

The possible values for direction are:

both	Netbios packets received on the interface rebroadcasted to other interfaces and netbios packets received on other interfaces are rebroadcasted into this interface. This is the default value.
disable	Netbios packets are not rebroadcasted into or out of this interface.

Example:

To enable rebroadcasting of netbios packets received by and sent from the interface "marketing":

```
Router-N(config-if:marketing) # ip netbios-rebroadcast both
```

ip ospf authentication-key

User level: privileged, supervisor.

Use the `ip ospf authentication-key` command to configure the interface authentication password.

Use the `no ip ospf authentication-key` command to remove the OSPF password.

The syntax for this command is:

```
[no] ip ospf authentication-key <key>
```

key	string (up to 8 characters)
-----	-----------------------------

Example:

```
Router-N(configure-if:marketing) # ip ospf authentication-key my_pass
```

ip ospf cost

User level: privileged, supervisor.

Use the `ip ospf` command to configure interface metric.

Use the `no ip ospf cost` command to set the cost to its default. The default is 1.

The syntax for this command is:

```
[no] ip ospf cost <cost>
```

cost	integer
------	---------

Example:

```
Router-N(configure-if:marketing) # ip ospf cost 10  
Done!
```

ip ospf dead-interval

User level: privileged, supervisor.

Use the `ip ospf dead-interval` command to configure the interval before declaring the neighbor as dead.

Use `no ospf dead-interval` to set the dead-interval to its default value of 40.

The syntax for this command is:

```
[no] ip ospf dead-interval <seconds>
```

seconds	Time in seconds (integer value)
---------	---------------------------------

Example:

```
Router-N(configure-if:marketing) # ip ospf dead-interval 15
```

ip ospf hello-interval

User level: privileged, supervisor.

Use this command to specify the time interval between OSPF hello messages the router sends.

Use `no ip ospf hello-interval` to set the hello-interval to its default.

The default is 10.

The syntax for this command is:

```
[no] ip ospf hello-interval <seconds>
```

seconds integer

Example:

```
Router-N(configure-if:marketing) # ip ospf hello-interval 5  
Done!
```

ip ospf priority

User level: privileged, supervisor.

Use the `ip ospf priority` command to configure interface priority used in DR election.

Use the `no ip ospf priority` to set the OSPF priority to its default value. The default is 1.

The syntax for this command is:

```
[no] ip ospf priority <priority>
```

priority integer

Example:

```
Router-N(configure-if:marketing) # ip ospf priority 17  
Done!
```

ip proxy-arp

User level: privileged, supervisor.

Use the `ip proxy-arp` command to enable proxy ARP on an interface.

Use the `no ip proxy-arp` command to disable proxy ARP on an interface.

The syntax for this command is:

```
[no] ip proxy-arp
```

Example:

To disable proxy ARP on interface marketing:

```
Router-N(config-if:marketing) #no ip proxy arp
```


ip redirects

User level: privileged, supervisor.

Use the `ip redirects` command to enable the sending of redirect messages on the interface.

Use the `no ip redirect` command to disable the redirect messages. By default, sending of redirect messages on the interface is enabled.

The syntax for this command is:

```
[no] ip redirect
```

Example:

```
Router-N(config-if:marketing) #ip redirects
```

ip rip authentication key

User level: privileged, supervisor.

Use the `ip rip authentication key` command to set the authentication string used on the interface.

Use the `no ip rip authentication key` command to clear the password.

The syntax for this command is:

```
[no] ip rip authentication key <password>
```

`password` The authentication string for the interface. Up to 16 characters are allowed.

Example:

To set the authentication string used on the interface “marketing” to be “hush-hush”.

```
Router-N(configure-if:marketing) # ip rip authentication  
key hush-hush
```

ip rip authentication mode

User level: privileged, supervisor.

Use the `ip rip authentication` command to specify the type of authentication used in RIP Version 2 packets.

Use the `no ip rip authentication` command to restore the default value of `none`.

The syntax for this command is: **[no] ip rip authentication mode**
[simple|none]

simple none	The authentication type used in RIP Version 2 packets:
	<ul style="list-style-type: none">• simple - clear text authentication.• none - no authentication.

Example:

To specify simple authentication to be used in RIP Version 2 packets on the interface "marketing".

```
Router-N(configure-if:marketing) # ip rip authentication  
mode simple
```

ip rip default-route-mode

User level: privileged, supervisor.

Use the `ip rip default-route-mode` command to enable learning of the default route received by the RIP protocol. The default state is `talk-listen`.

Use the `no ip rip default-route-mode` command to disable learning of the default route.

The syntax for this command is:

```
ip rip default-route-mode <mode>
```

The possible default route modes on an interface are:

talk-listen	Set RIP to send and receive default route updates on the interface.
talk-only	Set RIP to send but not receive default route updates on the interface.

Example:

```
Router-N(configure-if:marketing) # ip rip default-route-  
mode talk listen  
Done!
```

ip rip poison-reverse

User level: privileged, supervisor.

① You can only access this command in interface mode.

Type **interface [name]** at the command prompt to enter interface mode if necessary.

Use the `ip rip poison-reverse` command to enable split-horizon with poison-reverse on an interface.

Use the `no ip rip poison-reverse` command to disable the poison-reverse mechanism.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Poison reverse updates explicitly indicate that a network or subnet is unreachable rather than implying they are not reachable. Poison reverse updates are sent to defeat large routing loops.

The syntax for this command is:

```
[no] ip rip poison-reverse
```

Example:

```
Router-N(configure-if:marketing) # ip rip poison-reverse  
Done!
```

ip rip rip-version

User level: privileged, supervisor.

Use the `ip rip rip-version` command to specify the RIP version running on the interface basis.

The syntax for this command is:

```
ip rip rip-version <version>
```

The possible versions of the RIP packets received and sent on an interface are:

- 1 RIP Version 1 packets
- 2 RIP Version 2 packets.

Example:

To specify that RIP version 2 should be running on the basis of the interface “marketing”:

```
Router-N(configure-if:marketing) # ip rip rip-version 2  
Done!
```

ip rip send-receive-mode

User level: privileged, supervisor.

Use the `ip rip send-receive` command to set the RIP Send and Receive mode on an interface. The default state is **talk-listen**.

The syntax for this command is:

```
ip rip send-receive-mode <mode>[<default route metric>]
```

mode	talk-listen - Set RIP to receive and transmit updates on the interface.
	talkdefault-listen - Set RIP to receive updates on the interface and send only a default route.
	listen-only – Set RIP to only receive updates on the interface and not transmit them.
default route metric	Integer value

Example:

To set the RIP Send and Receive mode on the interface “marketing” to be listen-only:

```
Router-N(configure-if:marketing) # ip rip send-receive-  
mode listen-only  
Done!
```

ip rip split-horizon

User level: privileged, supervisor.

Use the `ip rip split-horizon` command to enable split-horizon mechanism. Use the `no ip rip split-horizon` command to disable the split-horizon.

By default split-horizon is enabled.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

The syntax for this command is:

```
[no] ip rip split-horizon
```

Example:

```
Router-N(configure-if:marketing) # no ip rip split-horizon  
Done!
```

ip routing-mode

User level: privileged, supervisor.

Use the `ip routing-mode` command to set the IP routing mode of the interface. In RT-MGMT mode, the interface functions as a routing interface. In RT_PRIMARY_MGMT mode, the interface function as both a routing interface and the primary management interface.

The IP address used in MSNM is the primary management interface IP address. Only one interface can be in RT_PRIMARY_MGMT mode. If no interface is configured to RT_PRIMARY_MGMT, the IP address used in MSNM is selected randomly.

The syntax for this command is:

```
ip routing-mode <mode>
```

mode RT-MGMT or RT_PRIMARY_MGMT mode

Example:

```
Router-N(config-if:marketing) #ip routing-mode  
RT_PRIMARY_MGMT
```

ip srrp backup

User level: privileged, supervisor.

Use the `ip srrp backup` command to backup an additional interface of the main router using the SRRP application. If the main router fails, the switch takes over its activities on all configured interfaces.

The syntax for this command is:

```
ip srrp backup <main router addr>
```

main router addr IP address of the main router interface

Example:

```
Router-N(config-if:marketing)#ip srrp backup 192.168.50.11
```

ip vlan/ip vlan name

User level: privileged, supervisor.

Use the `ip vlan` and `ip vlan name` commands to specify the VLAN on which an IP interface resides. You can specify either the VLAN ID using the `ip vlan` command or the VLAN name using the `ip vlan name` command.

The `no ip vlan` or `no ip vlan name` command to reset the IP interface to the default VLAN.

The syntax for this command is:

```
[no] ip vlan <vlan-id>
```

or

```
ip vlan name <vlan-Name>
```

Example:

To specify VLAN developmental as the VLAN used by interface “products”:

```
Router-N(config-if:marketing)# ip vlan name developmental
```

- ① If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

ip vrrp

User level: privileged, supervisor.

Use the `ip vrrp` command to create a virtual router on the interface.

Use the `no ip vrrp` command to delete a virtual router.

The syntax for this command is:

```
[no] ip vrrp <vr-id>
```

`vr-id` Virtual Router ID (1-255)

Example:

```
Router-N(configure-if:marketing) # ip vrrp 1
Done!
```

ip vrrp address

User level: privileged, supervisor.

Use the `ip vrrp address` command to assign an IP address to the virtual router.

Use the `no ip vrrp address` command to remove an IP address from a virtual router.

The syntax for this command is:

```
[no] ip vrrp <vr-id> address <ip-address>
```

`vr-id` Virtual Router ID (1-255)

`ip-address` The IP address to be assigned to the virtual router.

Example:

To assign address 10.0.1.2 to virtual router 1:

```
Router-N(configure-if:marketing) # ip vrrp 1 address
10.0.1.2
Done!
```

ip vrrp auth-key

User level: privileged, supervisor.

Use the `ip vrrp auth-key` command to set the virtual router simple password authentication for the virtual router ID.

Use the `no ip vrrp auth-key` command to disable simple password authentication for the virtual router instance.

The syntax for this command is:

```
[no] ip vrrp <vr-id> auth-key <key-string>
```

vr-id	Virtual Router ID (1-255)
key-string	Simple password string.

Example:

To assign “secret” as the simple password for virtual router 1:

```
Router-N(configure-if:marketing) # ip vrrp 1 auth-key  
secret  
Done!
```

ip vrrp override addr owner

User level: privileged, supervisor.

Use the `ip vrrp override addr owner` command to accept packets addressed to the IP address(es) associated with the virtual router, such as ICMP, SNMP, and TELNET (if it is not the IP address owner).

Use the `no ip vrrp override addr owner` command to discard these packets.

The syntax for this command is:

```
[no] ip vrrp <vr-id> override addr owner
```

vr-id	Virtual Router ID (1-255)
-------	---------------------------

Example:

```
Router-N(configure-if:marketing) # ip vrrp 1 override addr  
owner  
Done!
```


ip vrrp preempt

User level: privileged, supervisor.

Use the `ip vrrp preempt` command to configure the router to preempt a lower priority master for the virtual router ID.

Use the `no ip vrrp preempt` command to disable preemption for the virtual router instance.

By default, preemption is enabled.

The syntax for this command is:

```
[no] ip vrrp <vr-id> preempt
```

vr-id Virtual Router ID (1-255)

Example:

```
Router-N(configure-if:marketing) # ip vrrp 1 preempt
Done!
```

ip vrrp primary

User level: privileged, supervisor.

Use the `ip vrrp primary` command to set the primary address that shall be used as the source address of VRRP packets for the virtual router ID.

Use the `no ip vrrp primary` command to return to the default primary address for the virtual router instance.

By default, the primary address is selected automatically by the device.

The syntax for this command is:

```
[no] ip vrrp <vr-id> primary <ip-address>
```

vr-id Virtual Router ID (1-255)

ip-address Primary IP address of the virtual router. This address should be one of the router addresses on the VLAN.

Example:

```
Router-N(configure-if:marketing) # ip vrrp 1 primary
192.168.66.23
Done!
```

ip vrrp priority

User level: privileged, supervisor.

Use the `ip vrrp priority` command to set the virtual router priority value used when selecting a master router.

Use the `no ip vrrp priority` command to restore the default value.

The syntax for this command is:

```
[no] ip vrrp <vr-id> priority <pri-value>
```

vr-id	Virtual Router ID (1-255)
pri-value	The priority value. The range is 1-254.

Example:

To set the priority value for virtual router 1 to ten:

```
Router-N(configure-if:marketing) # ip vrrp 1 priority 10  
Done!
```

Example:

To set the virtual router simple password for virtual router 1 to abcd:

```
Router-N(configure-if:marketing) # ip vrrp 1 auth-key abcd  
Done!
```

ip vrrp timer

User level: privileged, supervisor.

Use the `ip vrrp timer` command to set the virtual router advertisement timer value (in seconds) for the virtual router ID.

Use `no ip vrrp timer` command to restore the default value.

The syntax for this command is:

```
[no] ip vrrp <vr-id> timer <value>
```

vr-id	Virtual Router ID (1-255)
value	The advertisement transmit time (seconds).

Example:

To set the virtual router advertisement timer value for virtual router 3 to 2:

```
Router-N(configure-if:marketing) # ip vrrp 3 timer 2  
Done!
```

Router RIP Context

- ① You can only access these commands in the “Router-RIP” context.
Type **router rip** at the command prompt to enter the “Router-RIP” context if necessary.

network

User level: privileged, supervisor.

Use the `network` command to specify a list of networks on which the RIP is running.

Use the `no network` command to remove an entry.

The syntax for this command is:

```
[no] network <ip-address> [<wildcard-mask>]
```

<code>ip addr</code>	The IP address of the network of directly connected networks
<code>wildcard-mask</code>	Wildcard mask address. Exists for compatibility with P550.

Example:

To specify that RIP will be used on all interfaces connected to the network 192.168.37.0:

```
Router-N(configure router:rip)# network 192.168.37.0  
Done!
```

redistribute

User level: privileged, supervisor.

Use the `redistribute` command to redistribute routing information from other protocols into RIP.

Use the `no redistribute` command to disable redistribution by RIP.

The default is disabled.

The syntax for this command is:

```
[no] redistribute <protocol>
```

<code>protocol</code>	Either Static or OSPF
-----------------------	-----------------------

Example:

```
Router-N(configure router:rip)# redistribute ospf  
Done!
```

timers basic

User level: privileged, supervisor.

Use the `timers basic` command to configure the route timer.

Use the `no timers basic` command to restore the timers to their default values.

The syntax for this command is:

```
timers basic <update><invalid>
```

<code>update</code>	RIP update timer in seconds (minimum = 30; default = 30)
<code>invalid</code>	RIP invalid route timer in seconds (minimum =30; default = 180)

- ① The Invalid Route Timer value must be larger than the Update Timer value. It is recommended that it be at least three times greater.
In any configuration all adjacent routers must have the same values for each of the timer parameters. It is possible to have different values for the timers on two adjacent routers, provided the Invalid Timer value is at least three times greater on one of the routers than the Update Timer value on the other router.

Example:

```
Router-N(configure router:rip)# timers basic 30 180
```

Router OSPF Context

- ① You can only access these command in the “Router-OSPF” context.
Type **router ospf** at the command prompt to enter the “Router -OSPF” context if necessary.

area

User level: privileged, supervisor.

Use the **area** command to configure the area ID of the router.

Use the **no area** command to deleted the area ID of the router (set it to 0) and remove the stub definition.

The default area is **0.0.0.0**.

- ① You cannot define a stub area when OSPF is redistributing other protocols or when the Area ID is 0.0.0.0.

The syntax for this command is:

```
[no] area <area id> [<stub>]
```

area id	IP address
stub	Stub

Example:

```
Router-N(configure router:ospf) # area 192.168.49.1
Router-N(configure router:ospf) # area 192.168.49.1 stub
```

network

User level: privileged, supervisor.

Use the **network** command to enable OSPF in this network.

Use the **no network** command to disable OSPF in this network.

The default is disabled.

The syntax for this command is:

```
network <net addr> [<wildcard-mask> [area <area id>]]
```

net addr	IP address
wildcard-mask	Wildcard mask address

area id Area ID. This parameter exists for compatibility with P550.

Example:

```
Router-N(configure router:ospf)# network 192.168.0.0  
Router-N(configure router:ospf)# area 192.168.0.0  
0.0.255.255 area 0.0.0.0
```

passive-interface

User level: privileged, supervisor.

Use the `passive interface` command to allow interfaces to be flooded into the OSPF domain as OSPF routes and not external routes.

- ① An interface becomes passive only if you use the `network` command to enable OSPF to run on the interface.

The syntax for this command is:

```
passive-interface <interface-name/net addr>
```

interface-name / Name of interface or IP address.
net addr

Example:

```
Router-N# passive-interface FastEthernet 1.10
```

redistribute

User level: privileged, supervisor.

Use the `redistribute` command to redistribute routing information from other protocols into OSPF.

Use the `no redistribute` command disables redistribution by OSPF.

The syntax for this command is:

```
[no] redistribute <protocol>
```

protocol

- static
- conneted
- RIP

Example:

```
Router-N(configure router:ospf)# redistribute static
```

timers spf

User level: privileged, supervisor.

Use the `timers spf` command to configure the delay between runs of OSPF's SPF calculation. Use the `no` form of this command to restore the default (3 seconds).

The syntax for this command is:

```
[no] timers spf <spf-holdtime>
```

<code>spf-holdtime</code>	The time in seconds of the delay between runs of OSPF's SPF calculation.
---------------------------	--

Example:

```
Router-N(configure router:rip)# timers spf 5  
Done!
```

Router SRRP Context

- ① You can only access these commands in the “Router-SRRP” context.
Type **router srrp** at the command prompt to enter the “Router -SRRP” context if necessary.

poll-interval

User level: user, privileged, supervisor

Use the `poll-interval` command to configure the polling interval in seconds used by SRRP.

Use the `no poll-interval` command to return to the default polling interval of 1 second.

The syntax for this command is:Syntax

```
[no] poll-interval <poll interval>
```

`poll interval` Poll interval (integer value, in seconds)

Example:

```
Router-N# poll-interval 4
```

timeout

User level: user, privileged, supervisor

Use the `timeout` command to configure the timeout (in seconds) after which SRRP declares the main router dead if it does not reply to polling.

Use the `no timeout` form command to return the timeout to default timeout interval of 12 seconds.

The syntax for this command is:

```
[no] timeout <timeout>
```

`timeout` An integer (in seconds)

Example:

```
Router-N# timeout 6
```

- ① The timeout should be at least twice as long as the interval.

Index of Layer 2 CLI Commands

C

clear cam 9
clear dynamic vlans 10
clear event-log 10
clear interface 11, 214
clear ip route 11, 214
clear logging file 10
clear logging server 11
clear port mirror 11
clear port static-vlan 12
clear power history 12
clear radius authentication server 12
clear rmon statistics 12
clear screen 13, 134
clear snmp trap 14
clear timezone 14
clear utilization cpu 14
clear vlan 15
configure 16, 216
copy 15, 17, 23, 25, 216, 217, 220
copy module-config scp 15
copy module-config tftp 16
copy running-config scp 17
copy scp module-config 19
copy scp stack-config 20
copy scp startup-config 22
copy stack-config scp 23
copy stack-config tftp 24
copy startup-config scp 25
copy tftp EW_archive 26
copy tftp l2-config 221
copy tftp module-config 27
copy tftp stack-config 27
copy tftp SW_image 29
crypto key generate dsa 31

D

dir 32

disable interface 31

disconnect ssh 33

G

get time 34

H

hostname 35

I

ip http enable 41

ip icmp redirect 41

ip ssh enable 42

ip telnet enable 43

ip telnet-client enable 42

N

no hostname 35, 226

no ip http 43

no ip icmp redirect 43

no ip ssh 44

no ip telnet 44

no ip telnet-client 44

no rmon alarm 45

no rmon event 45

no rmon history 46

no snmp-server 46

no snmp-server community 46

no snmp-server engineID 47

no snmp-server group 47

no snmp-server host 48

no snmp-server notifications 49

no snmp-server remote-user 49

no snmp-server user 49

no snmp-server view 50

no username 50

nvrn initialize 51

P

ping 163

R

reset 52, 239

rmon alarm 55

rmon event 56

rmon history 56

S

session 57, 242

set allowed managers 58

set allowed managers ip 58

set arp-aging-interval 59

set arp-tx-interval 59

set autopartition 60

set boot bank 199

set cascading 61

set device-mode 61

set inband vlan 65

set intelligent-multicast 65

set intelligent-multicast client port pruning time 65

set intelligent-multicast group filtering delay time 66

set intelligent-multicast router port pruning time 66

set interface inband 67

set interface outband 67

set interface ppp 67

set interface ppp enable/disable/off/reset 68

set intermodule port redundancy 69

set intermodule port redundancy off 70

set internal buffering 70

set ip route 71

set license 71

set logging file condition 72

set logging file disable 74

set logging file enable 74

set logging server 74

set logging server access-level 75

set logging server condition 75

set logging server disable 77

set logging server enable 77

set logging server facility 78

set logging session condition 79

set logging session disable 80

set logging session enable 80

set logout 81

set outband speed 82

set port auto-negotiation-flowcontrol-advertisement 82

set port channel 83

set port classification 84

set port disable 84

set port duplex 89

set port enable 91

set port flowcontrol 91

set port level 92

set port mirror 93

set port name 94

set port negotiation 94

set port redundancy 96, 97

set port redundancy on/off 97

set port redundancy-intervals 99

set port security 99

set port spantree 99

set port spantree cost 99

set port spantree priority 101

set port speed 101

set port static-vlan 102

set port trap 103

set port vlan 103

set port vlan-binding-mode 104

set ppp authentication incoming 105

set ppp baud-rate 106

set ppp chap-secret 106

set ppp incoming timeout 106

set radius authentication retry-time 109

set radius authentication secret 110

set radius authentication server 110

set radius authentication udp-port 110

set security mode 112

set security violation 112

set snmp community 113

set snmp retries 113

set snmp timeout 114

set snmp trap 114

set snmp trap auth 115

set spantree 116

set spantree priority 118

set system contact 119, 120, 244, 245

set system location 120, 245

set system name 121, 246

- set terminal recovery password disable 121
- set terminal recovery password enable 121
- set time client 122
- set time protocol 122
- set time server 123
- set timezone 123
- set trunk 124
- set utilization cpu 124
- set vlan 125
- set web aux-files-url 125
- show
 - timezone** 194
 - show allowed managers status 127
 - show arp-aging-interval 127, 128
 - show arp-tx-interval 128
 - show autopartition 129
 - show boot bank 199
 - show cam 130
 - show cam mac 131, 132
 - show cam vlan 131
 - show cascading fault-monitoring 132
 - show dev log file 133
 - show device-mode 134, 248
 - show download status 134
 - show dynamic vlans 135
 - show image version 135
 - show intelligent-multicast 135
 - show intelligent-multicast hardware-support 136
 - show interface 137
 - show intermodule port redundancy 137
 - show internal buffering 137
 - show ip route 141, 258
 - show ip ssh 142
 - show license 142
 - show log 208
 - show logging file condition 150
 - show logging file content 151
 - show logging server condition 153
 - show logging session condition 154
 - show module 154
 - show module identity 156
 - show port 157
 - show port auto-negotiation-flowcontrol 158
 - show port classification 160
 - show port flowcontrol 164
 - show port mirror 166
 - show port redundancy 166
 - show port security 167
 - show port trap 168
 - show port vlan-binding-mode 168
 - show ppp authentication 171
 - show ppp baud-rate 172
 - show ppp configuration 172
 - show ppp incoming timeout 172
 - show ppp session 173, 174
 - show protocol 173
 - show radius authentication 174
 - show rmon alarm 173, 174
 - show rmon event 176
 - show rmon history 176
 - show rmon statistics 177
 - show secure access 178
 - show secure mac 178
 - show security mode 179
 - show snmp 179
 - show snmp engineID 181
 - show snmp group 182
 - show snmp retries 184
 - show snmp timeout 184
 - show snmp user 184
 - show snmp userToGroup 185
 - show snmp view 186
 - show spantree 188
 - show system 191, 270
 - show system-log 191
 - show tftp download software status 192
 - show time 192
 - show time parameters 193
 - show timeout 149, 193
 - show trunk 194
 - show upload status 195
 - show username 196
 - show utilization 196
 - show vlan 198
 - show web aux-files-url 199
 - snmp-server community 199
 - snmp-server enable 200

snmp-server enable notifications 200

snmp-server engineID 200

snmp-server group 201

snmp-server host 202

snmp-server informs 203

snmp-server remote-user 204

snmp-server user 205

snmp-server view 206

sync time 207

T

tech 207

telnet 207

terminal 9

U

username 208

Index of Layer 3 CLI Commands

area 309
arp 212
arp timeout 212
clear arp-cache 213
clear fragment 214
clear ip route 214
clear ip traffic 215
clear screen 215
clear vlan 215
configure 216
copy module-config scp 216
copy module-config tftp 217
copy running-config scp 218
copy running-config startup-config 219
copy running-config tftp 219
copy scp module-config 220
copy scp startup-config 221
copy startup-config scp 221
copy startup-config tftp 222
copy tftp startup-config 223
default-metric 290
enable vlan commands 290
erase startup-config 223
event clear 223
event log 224
event set 225
event show 226
exit 226
fragment chain 226
fragment size 227
fragment timeout 227
help 228
hostname 228
icmp in-echo-limit 229
interface 229
ip access-default-action 230
ip access-group 230
ip access-list 231
ip access-list-cookie 232
ip access-list-copy 232
ip access-list-dscp operation 233
ip access-list-dscp trust 233
ip access-list-name 234
ip access-list-owner 235
ip address 291
ip admin-state 291
ip bootp-dhcp network 292
ip bootp-dhcp relay 235
ip bootp-dhcp server 292
ip broadcast-address 293
ip default-gateway 236
ip directed-broadcast 293
ip icmp-errors 236
ip max-arp-entries 237
ip max-route-entries 238
ip netbios-rebroadcast 294
ip netmask-format 238
ip ospf authentication-key 294
ip ospf cost 295
ip ospf dead-interval 295
ip ospf hello-interval 295
ip ospf priority 296
ip proxy-arp 296
ip redirects 297
ip rip authentication key 297
ip rip authentication mode 298
ip rip default-route-mode 298
ip rip poison-reverse 299
ip rip rip-version 299
ip rip send-receive-mode 300
ip rip split-horizon 301
ip route 239
ip routing 240
ip routing-mode 301

ip simulate 240
ip srrp backup 302
ip unicast cache aging 241
ip unicast cache aging timeout 241
ip unicast cache high-limit 242
ip unicast cache update-timeout 242
ip vlan/ip vlan name 302
ip vrrp 303
ip vrrp address 303
ip vrrp auth-key 304
ip vrrp override addr owner 304
ip vrrp preempt 305
ip vrrp primary 305
ip vrrp priority 306
ip vrrp timer 306
network 307
network 309
passive-interface 310
ping 243
poll-interval 312
prompt-length 244
redistribute 307
redistribute 310
reset 244
rmon2 auto-learn 247
rmon2 filters 247
rmon2 host 245
rmon2 matrix 245
rmon2 protocol-dir 248
rmon2 protocol-dist 246
rmon2 subnets 246
Router Configuration Contexts 211
router ospf 248
router ip 249
router srrp 249
router vrrp 250
session 250
set device-mode 251
set policy type 252
set qos dscp-cos-map 252
set qos dscp-name 253
set qos policy-source 253
set system contact 254
set system location 255
set system name 255
set vlan 256
Shortcuts to Commands by Context 211
show copy status 256
show device-mode 257
show download status 257
show dscp 258
show erase status 258
show fragment 259
show ip access-group 259
show ip access-list-dscp 262
show ip access-lists 260
show ip access-lists details 260
show ip access-list-summary 262
show ip arp 263
show ip icmp 264
show ip interface 264
show ip interface brief 265
show ip ospf 266
show ip ospf database 266
show ip ospf interface 267
show ip ospf neighbor 267
show ip protocols 268
show ip reverse-arp 269
show ip route 269
show ip route best-match 270
show ip route static 270
show ip route summary 271
show ip srrp 271
show ip traffic 272
show ip unicast cache 273
show ip unicast cache aging timeout 277
show ip unicast cache host 274
show ip unicast cache networks 275
show ip unicast cache networks detailed 275
show ip unicast cache nextHop 276
show ip unicast cache summary 276
show ip vrrp 277
show ip vrrp detail 278
show policy type 279
show rmon2 auto-learn 283
show rmon2 filters 283
show rmon2 host 281
show rmon2 host-top-n 284

show rmon2 matrix 282
show rmon2 matrix-top-n 284
show rmon2 protocol-dist 280
show rmon2 protocol-dist-top-n 285
show rmon2 state 280
show rmon2 subnets 282
show rmon2 subnet-top-n 285
show startup-config 286
show system 286
show upload status 287
show vlan 287
terminal 287
timeout 312
timers basic 308
timers spf 311
traceroute 288
validate-group 288

